社保 SmartCOS®使用手册

Version 1.5（修订版）



深圳市明华澳汉科技股份有限公司

2002 年 10 月

前　　言

随着电子技术的发展，集成电路（IC）卡的应用得到了社会各界的广泛重视。中国劳动和社会保障部也于 2000 年 6 月颁布了《社会保障（个人）卡规范》。作为国内制卡行业的先锋，深圳市明华澳汉科技有限公司开发出了符合《规范》及 ISO/IEC 7816 的、具有自主版权的社保 SmartCOS V1.5 以支持《规范》，提高集成电路（IC）卡在国内的应用和开发水平，为振兴民族产业作出一份贡献。

明华公司也希望国内外在芯卡操作系统领域有一定见解的专家、学者及同行和我们共同探讨、交流，从而提高国内芯卡操作系统的应用、开发水平。

目录

1、 社保 SMARTCOS V1.5 简介 1

1.1、 应用领域 1
1.2、 内部结构 1
1.3、 功能模块化划分 2
1.3.1、 数据传输......2
1.3.2、 保密通信......2
1.3.3、 命令解释......3
1.3.4、 文件管理器......3

2、 文件系统 4

2.1、 文件系统的组织结构 4
2.2、 基本文件结构 5
2.3、 基本文件类型 6
2.4、 文件访问方式 7
2.5、 文件的空间结构 9
2.6、 文件类型、密钥类型及相关命令 9
2.7、 文件短标识符与文件名称 10

3、 社保 SMARTCOS V1.5 的安全系统 12

3.1、 状态机 12
3.2、 安全属性和状态机的关系 12
3.3、 状态机转变机制 13
3.4、 密码算法 13

4、 复位应答 14

5、 基本命令集 15

5.1、 命令与应答机制 15
5.2、 命令与应答编码 16

6、 命令描述 18

6.1、 CREATE FILE 建立文件 18
6.2、 WRITE KEY 增加或修改密钥 23
6.3、 GENERATE KEY 生成子密钥或过程密钥 29
6.4、 CRYPT 安全模块命令 31
6.5、 APPLICATION BLOCK 应用锁定 33
6.6、 APPLICATION UNBLOCK 应用解锁 35
6.7、 CARD BLOCK 卡片锁定 36
6.8、 EXTERNAL AUTHENTICATION 外部认证......37
6.9、 GET CHALLENGE 产生随机数 39
6.10、 GET RESPONSE 取响应......40

6.11、 INTERNAL AUTHENTICATION 内部认证 41
6.12、 PIN CHANGE/UNBLOCK 个人密码的解锁 42
6.13、 READ BINARY 读二进制 44
6.14、 READ RECORD 读记录 45
6.15、 SELECT FILE 选择文件 47
6.16、 UPDATE BINARY 修改二进制 49
6.17、 UPDATE RECORD 修改记录 51
6.18、 VERIFY 校验 53
6.19、 CHANGE PIN 修改 55
6.20、 UNBLOCK 解锁口令 57
6.21、 INITIALIZE FOR LOAD 帐户划入初始化 59
6.22、 CREDIT FOR LOAD 帐户划入 61
6.23、 INITIALIZE FOR PURCHASE 消费初始化 63
6.24、 DEBIT FOR PURCHASE 消费 65
6.25、 GET BALANCE 读余额 67
6.26、 GET CARDDATA 取卡片数据 68
6.27、 GET TRANSACTION PROVE 取交易认证 69
6.28、 UPDATE/GET STARTING DAY 修改/读取年度起始日期 71

7、 安全机制 72

7.1、 加密算法 72
7.2、 密钥管理 73
7.2.1、 共存应用 73
7.2.2、 密钥的独立性 73
7.2.3、 密钥的生成 73
7.2.4、 密钥装载 73
7.2.5、 密钥访问 74
7.2.6、 密钥属性 74
7.2.7、 密钥的使用和存放 76
7.2.8、 密钥的终止 76
7.3、 安全报文 77
7.3.1、 报文完整性和验证 77
7.3.2、 安全报文传送的命令情况 78
7.4、 数据的加、解密计算 80
7.4.1、 数据加密计算 80
7.4.2、 数据解密计算 81
7.5、 ED/EP 应用的密钥关系 83
7.5.1、 密钥关系表 83
7.5.2、 子密钥推导方法 83
7.5.3、 过程密钥的产生 84

8、 用户卡发卡流程 86

9、 医疗消费交易流程 87

1、 社保 SmartCOS V1.5 简介

1.1、 应用领域

社保 SmartCOS V1.5 有如下特点：

1. 符合《社会保障（个人）卡规范》。
2. 数据文件支持二进制文件、定长记录文件、变长记录文件、循环定长记录文件。
3. 支持 DES、Triple DES 等加密算法，并支持用户特有的安全加密算法的下载。
4. 支持线路加密、线路保密功能，防止通信数据被非法窃取或篡改。
5. 可用作安全保密模块，使用过程密钥实现加密、解密。
6. 支持符合 ISO-7816-3 标准的 T=0 通讯协议。
7. 卡片支持多种容量选择,可选择 2K、4K、8K、16K、32K 等字节的 EEPROM 空间。
8. 安全机制使用状态机，并支持 PIN 检验、KEY 认证、数据加密、解密、MAC 验证。
9. 支持防插拔功能。

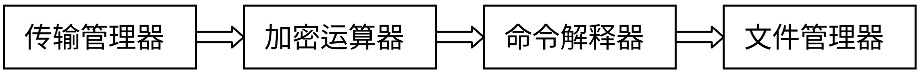
1.2、 内部结构

SMARTCOS 的内部结构组成如下：CPU 及加密逻辑、RAM、ROM、EEPROM 及 I/O 五部分组成，是一个完整的计算机安全体系。用户数据放在被加密逻辑保护的 EEPROM 中，COS 掩膜在 ROM 中以保证代码安全。COS 将用户的过程密钥生成后放在 RAM 空间中，掉电后自动丢失，保证其安全性。

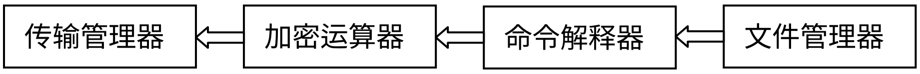
1.3、 功能模块化划分

社保 SmartCOS V1.5 的基本操作方式为：从接口设备接收一条命令，然后经过处理返回应答信息给接口设备。其处理过程如下图所示：

命令处理过程：



命令应答过程：



每条命令的处理都要经过上述四个模块，如果其中的任意一个模块在处理中发现错误都将返回相应的出错信息。

1.3.1、 数据传输

传输管理器负责智能卡和接口设备之间的数据通信，接收过程中要处理对输入数据的缓冲，响应过程控制数据的发送。通信使用的协议是 ISO7816-3 所规定的 T=0 的异步半双工字符传输协议。

当接口设备给卡上电之后，首先由卡发送一个遵守《社会保障（个人）卡规范》的复位应答信息（ATR）给接口设备，然后接口设备发送命令头来启动命令处理过程。传输管理器在正确地接收到命令后交给下一个功能模块进行处理，最后还要把该命令的执行结果返回给接口设备。

1.3.2、 保密通信

数据在传输方式上有四种类型：明文方式、明文校验方式、密文方式和密文校验方式。对以明文方式进行传输的数据由传输管理器直接送给命令处理模块。当数据以明文校验方式、密文方式和密文校验方式传输时需要加密运算器对数据进行处理。

1.3.3、 命令解释

命令解释器对外部输入的每条命令做语法分析，分析和检查命令参数是否正确，然后根据命令参数的含义执行相应的功能模块。如果发现参数有错，将从该模块直接返回错误信息。

1.3.4、 文件管理器

文件管理器控制对文件的操作和访问。在做数据操作前，文件管理器将根据文件的安全属性检查卡的安全状态，以确定操作的可行性。文件的安全属性和文件结构一旦产生便处于文件管理器的控制之下。

对文件数据的操作和管理将按照如下的规则：

1．对某个文件做操作之前，必须先选择该文件。

2．文件系统的三层结构，并且操作系统不支持以路径方式选择文件，所以在选择某个文件前必须先选择它的上一层文件，不允许跨层选择。卡片上电后自动选择主控文件。

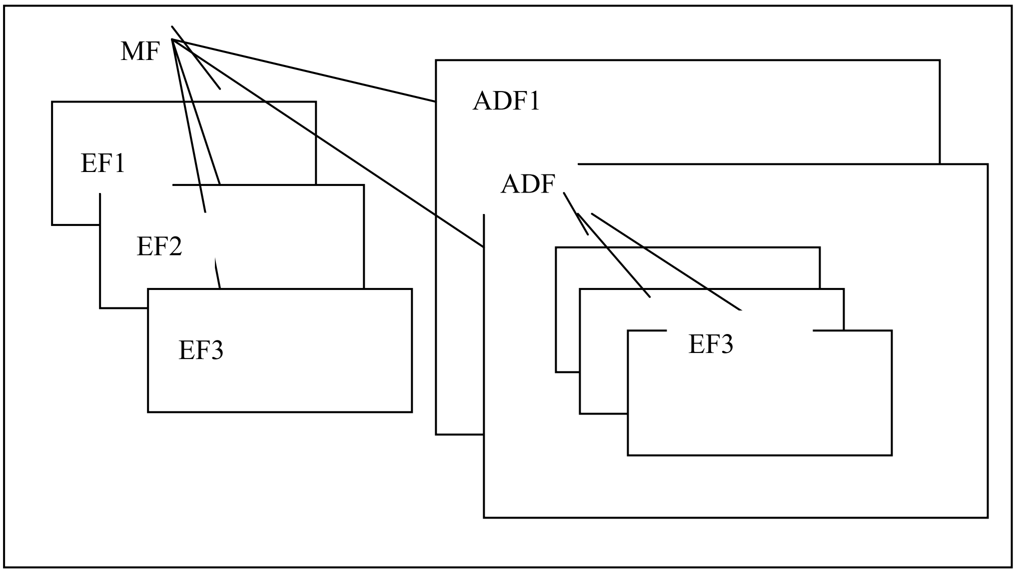
3．访问文件中的数据要受文件的安全属性的控制。

4．对文件的建立要受该文件所属的上层文件的安全属性的控制。

2、 文件系统

2.1、 文件系统的组织结构

社保 SmartCOS V1.5 的文件系统是完全遵照《中国金融集成电路 IC 卡规范及应用规范》和 ISO/IEC 7816-4 来组织的，具体的层次结构如下图所示：



1. 主控文件(Master File , MF)

主控文件是整个文件系统的根（可看做根目录），每张卡有且只有一个主控文件。它是在卡的个人化过程中首先被建立起来的，在卡的整个生命周期内一直存在并保持有效，可存储卡的公共数据信息并为各种应用服务。由个人化建立起来的主控文件包括文件控制参数以及文件安全属性等信息。在物理上，主控文件占有的存储空间包括 MF 文件头的大小以及 MF 所管理的 EF 和 DF 的存储空间。

2. 专用文件(Dedicated File，DF)

在 MF 下针对不同的应用建立起来的一种文件，是位于 MF 之下的含有 EF 的一种文件结构（可看做文件目录），它存储了某个应用的全部数据以及与应用操作相关的安全数据。

DF 由创立文件命令建立。对 DF 的建立操作由 MF 下建立文件的安全属性

控制。

在 DF 下面不可再建立子 DF，只能建立 EF

为了保证各个 DF 的相互独立，只能从文件系统的 MF 层次选择一个 DF，对 DF 下的数据进行的操作由各当前系统的状态机控制。

3. 基本文件(Elementary File，EF)

基本文件存储了各种应用的数据和管理信息，它存在于 MF 和 DF 下。EF 从存储内容上分为两类：安全基本文件和工作基本文件。

安全基本文件(Secret Elementary File，SEF)的内容包含用于用户识别和与加密有关的保密数据(个人识别码、密钥等)，卡将利用这些数据进行安全管理。SEF 要在 MF 或 DF 建立后，才能建立。建立后每个 KEY 都可以定义不同的修改权限。安全基本文件的内容不可被读出，但可使用专门的指令来写入和修改。在 MF 和每个 DF 下只能建立 1 个安全基本文件，但每个文件中的 KEY 和 PIN 的类型由用户指定。

工作基本文件(Working Elementary File，WEF)包含了应用的实际数据，其内容不被卡解释。在符合 WEF 的读、修改安全属性时，可对其内容进行读取、修改。工作文件的个数和大小受到 MF 或 DF 所拥有空间的限制。

整个文件系统的空间在 MF、DF 和 EF 建立时被分配和确定，以后在物理上不会发生变化。当访问 EF 时，必须先选择相应的 MF 或 DF。

可以从文件系统的任何位置选择 MF。

2.2、 基本文件结构

根据 ISO/IEC 7816-4 和《社会保障（个人）卡规范》有关基本文件结构的定义，社保 SmartCOS V1.5 支持下列四种基本文件结构：

1．二进制结构

二进制文件为一个数据单元序列，数据以字节为单位进行读写，其中的数

据结构则由应用解释。

2．线性定长记录文件结构

在这种记录结构中，每条记录的长度都是相同的。通过记录号或记录标识可以访问这类记录。记录号和记录标识的长度为 1 个字节，取值范围是‘01’至‘FE’。‘00’表示当前记录，‘FF’为系统保留。每次访问都是以整条记录为单位进行操作的，而且必须严格遵守记录长度的规定。

3．线性变长记录文件结构

在这类结构中，每条记录的长度可以各不相同。对线性变长记录的访问与访问线性定长记录的方法相同。对于变长记录文件，社保 SmartCOS V1.5 内部采用 LV 格式。

4．循环定长记录文件结构

这是一类特殊的定长记录文件结构。在逻辑上，这类文件可看作一个环形记录队列，记录按照先进先出的原则存储。添加记录时，最新一次写入的记录的记录号为 1，上一次写入的记录的记录号为 2，依次类推。记录的个数与预留的记录空间的大小以及记录的长度相关，记录个数=记录空间大小整除记录长度。

此外社保 SmartCOS V1.5 还有一些只能特殊使用的文件类型，如 ATR、密钥文件、医疗保险个人帐户文件等，但其文件结构也不超除以上四种文件的类型。

2.3、 基本文件类型

根据 ISO/IEC 7816-4、《社会保障（个人）卡规范》有关基本文件结构的定义，SMARTCOS 支持下列文件类型：

文件类型说明表如下：

文件类型								类型描述
B7	**B6**	**B5**	**B4**	**B3**	**B2**	**B1**	**B0**	状态
0	0							文件数据以明文形式写入
0	1							文件数据以明文+MAC 形式写入

1	0							文件数据以密文形式写入
1	1							文件数据以密文+MAC 形式写入
		0	0	0	0	0	0	二进制
		0	0	0	0	0	1	定长记录
		0	0	0	0	1	0	变长记录
		0	0	0	0	1	1	循环定长
		0	0	0	1	0	0	ATR 文件
		0	0	0	1	0	1	密钥文件
		0	0	0	1	1	0	医疗保险个人帐户文件
其他值								系统保留

2.4、　文件访问方式

1．主文件 MF

复位后自动被选择，在任何一级子目录下可通过文件标识 3F00 或其文件名来选择 MF

2．专用文件 DF

通过文件名或文件标识符来选择 DF，在 MF 下可以选择任意 DF。如果当前文件是一个 DF 下的一个 EF，同样可以通过选择 DF 的文件标识符或文件名来选择任意 DF。

3．二进制文件

在满足读条件时可使用 Read Binary 读取，在满足写条件时可用 Update Binary 来更改二进制文件的内容。

4．定长记录文件

在满足读条件时可使用 Read Record 读取，在满足写条件时可用 Update Record 来更改指定记录的内容。

5．循环定长记录文件

在满足读条件时可使用 Read Record 读取，在满足写条件时可用 Update Record 来更改指定记录的内容。

当记录写满后自动覆盖最早写的记录，最后一次写入的记录，其记录号总

是 1，上次写入的记录号是 2，依次类推。

6．变长记录文件

在满足读条件时可使用 Read Record 读取，在满足写条件时可用 Update Record 来更改指定记录的内容。

7．ATR 文件

ATR 文件是存在于 MF 下的一个二进制文件，其内容是卡上电复位信息。如果不建立，则上电复位返回社保 SmartCOS V1.5 的缺省值。在满足 ATR 文件写条件时，可用 Update Binary 来写入或更改 ATR 文件的内容。在满足读条件时，可使用 Read Binary 读取 ATR 文件的内容。

8．　医疗保险个人帐户文件

医疗保险个人帐户文件是 SmartCOS 内部文件，其文件的大小及读写权限均由 SmartCOS 内部设定。外界只能通过帐户划入、医疗消费专用命令，由 SMARTCOS 内部对其进行读写。此文件在医疗消费应用中必须被建立，且每个医疗消费应用下只能有一个。

9．KEY 文件及其文件中的密钥

每个 DF 或 MF 下有且只有一个 KEY 文件，在任何情况下密钥均无法读出。一旦离开该目录，该目录下的所有权限将全部丢失。

在 KEY 文件中可存放多个密钥，每个密钥为一条定长记录。记录中规定了其标识、版本、算法、属性及密钥本身等相关内容。

在满足 KEY 文件的增加权限时可用 Write KEY 命令增加一条记录；只有在满足某个密钥的使用权限时才可以使用该密钥；在满足某个密钥的修改权限时才可以修改该密钥。

每种密钥具有其独立性，用于一种特定功能的密钥不可作为它用。社保 SmartCOS V1.5 支持以下几种密钥：

密钥类型表如下所示：

KEY 类型	该类型 KEY 作用描述
00	消费取现密钥

01	帐户划入密钥
02	TAC 密钥
05	应用维护密钥，用于产生应用锁定、应用解锁、卡片锁定、卡片锁定和计算读、更新二进制、记录命令的 MAC
08	外部认证密钥，用于外部认证过程
09	内部认证密钥，用于内部认证过程
0B	个人密码（PIN），用于个人密码校验
0C	超级 PIN，用于解锁、修改 PIN
其它	系统保留

2.5、 文件的空间结构

社保 SmartCOS V1.5 整个的文件空间划分如下：

当你建立完 MF 之后，SMARTCOS 1.0 自动将整个 EEPROM 空间都分配给它。MF 的文件头长度为 10 个字节+文件名长度（5-16 个字节）。

每个 DF 所占空间=DF 文件头空间（等同于 MF）+DF 下所有的文件空间之和。

二进制结构文件的空间=文件头空间（11 个字节）+EF 所申请的空间。

定长记录和循环定长记录文件的空间=文件头空间（11 个字节）+记录数 X 记录长度。

变长记录结构文件的空间=文件头空间（11 个字节）+建立时申请的空间。

安全基本文件的空间=文件头空间（11 个字节）+密钥个数 X（25 个字节）

2.6、 文件类型、密钥类型及相关命令

MF 在个人化的过程中首先被建立，且文件标识符固定为 3F 00，在其建立之后，如果要建立自己的复位信息文件（ATR 文件）则必须首先被建立，长度最大为 11 个字节，其内容必须符合人行规范和 ISO/IEC 7816-4，否则某些终端可能不能识别，其后建立的必须是安全文件。在 DF 下首先被建立的是安全文件。相关性参见下表：

	主控文件MF	专用文件DF	二进制文件(00)	定长记录(01)	循环文件(03)	变长文件(02)	ATR文件(04)	钱包文件(06)	存折文件(07)	安全文件(05)
Create File	√	√	√	√	√	√	√	√	√	√
Write KEY										√
Read Binary			√				√			
Update Binary			√				√			
Read Record				√	√	√				
Append Record				√	√	√				
Update Record				√		√				
Select File	√	√	√	√	√	√	√			
Credit For Load								√	√	
Debit For Purchase/Case Withdraw								√	√	
Debit For Unload									√	
Get Balance								√	√	
Update Overdraw Limit									√	

2.7、 文件短标识符与文件名称

2.7.1 文件标识

文件标识（File Identifier，‘FID’）是文件的标识代码，用 2 个字节表示。文件标识是用户在建立文件时自己定义的。同一个目录下的文件标识必须是唯一的。所有文件都有其文件标识，并可通过文件标识用 Select File 命令进行选择。具体应用可参见本手册第 6 章对 Select File 命令的描述。

2.7.2 短文件标识

短文件标识（short EF identifier，‘SFI’）只有五位，取值范围为 1~30。同一个目录下的短文件标识必须是唯一的。短文件标识不能作为文件标识或文件名用 Select File 命令选择文件。

应用短文件标识查找文件的命令有：Read Binary、Update Binary 、Read

Record、Update Record。具体使用可参见本手册第 6 章对以上各条命令的描述。

2.7.3 文件名

文件名是某一个具体应用的名称。因此只有 MF 和 DF 才有文件名且文件名可以不唯一。同文件标识一样，文件名也是由用户在建立文件时自己定义的。SMARTCOS 规定文件名的长度应为 5～16 个字节。MF 和 DF 又可通过其文件名用 Select File 命令进行选择，具体应用可参见本手册第 6 章对 Select File 命令的描述。

不论用以上哪种方式选择文件，只要选择成功，该文件就被置为当前文件。

3、 社保 SmartCOS V1.5 的安全系统

社保 SmartCOS V1.5 的安全体系有以下几个阶段：在芯片制造商完成芯片的制造后，SMARTCOS 处于未初始化状态，卡片制造厂商封装完成后进行卡片初始化和检测，此时 SMARTCOS 处于初始化阶段，初始化和检测完成后 SMARTCOS 卡处于未个人化阶段。将卡提交给发卡方后，发卡方需正确地使用个人化密钥后才能个人化，这样可保证卡在运输过程中的安全。个人化开始后 SMARTCOS 处于个人化阶段，这个过程中发卡方设计自己应用的安全体系并下装到卡中，当个人化过程结束后，SMARTCOS 将在发卡方规划的安全体系的保护下对《规范》和 ISO/IEC7816-3/4 中的指令进行解释和执行。

在进行安全体系的规划过程中须理解社保 SmartCOS V1.5 安全体系中以下几个概念：状态机、安全属性和状态机的关系、状态机跳变机制和密码算法。

3.1、 状态机

状态机又称安全状态，是指卡在当前所处的一种安全级别。卡的主控目录和当前应用目录分别具有 16 种不同的安全状态。在卡内部用一个寄存器的高四位表示主控目录的安全状态，其表示整个卡所处的安全级别。寄存器低四位表示当前应用的安全状态。安全状态共 16 种，即 0-F 种的一种。主控目录的安全状态复位后为 0，应用目录的改变不改变主控目录的安全状态，只有主控目录下的口令核对或外部认证才能改变主控目录的安全状态。

当前应用的安全状态在被成功地选择或复位后自动清为 0。只能用当前应用的口令核对或外部认证才能改变当前应用的状态。如当前的目录为 MF，则当前应用的安全状态等于主控目录的安全状态。

3.2、 安全属性和状态机的关系

安全属性是指对某个文件进行某种操作时必须达到的状态机，又称其为访

问权限，一种访问权限是在建立该文件时指定的。社保 SmartCOS V1.5 的访问权限具有其独特性，是一个状态机区间来描述一种权限的。比如描述一个文件的读权限为 XY，则其访问权限为：当前应用的状态机 M 必须满足：X=<M=<Y。

因此，若要定义一种永远不能获得的权限的方法为，定义该安全属性为 XY(X>Y),即可。

如果定义一种权限可自动获得则定义该权限为 0X 即可。因为复位后的主控文件和成功选择后的应用的安全状态都为 0，0 是一种自动获得的状态机。

3.3、 状态机转变机制

社保 SmartCOS V1.5 通过核对口令和外部认证两种方法来实现状态机的转变。在同一个应用下，状态机一经获得则一直被保存直到从这一应用下退出。

3.4、 密码算法

社保 SmartCOS V1.5 支持 Single DES、Triple DES 算法。算法完全遵照《社会保障(个人)卡规范》，所以关于该算法的使用方法请参考《社会保障(个人)卡规范》即可。

本手册第 7 部分也对密码算法作了陈述。

4、 复位应答

对于 T=0 通讯协议的卡，在个人化时没有建立 ATR 文件，则缺省的复位应答信息如下表：

符号	字节内容	内容解释
TS	3B	正向约定
T0	6D	TB1 和 TC1 存在，历史字符为 12 个
TB1	00	无需额外的编程电压
TC1	02	需 2 个额外的保护时间
T1-TD	XX	历史字符

SMARTCOS 历史字符的特定意义：

符号	字节内容	内容解释
T1-T2	XXXX	芯片提供机构注册标识号
T3	XX	EEPROM 容量
T4	XX	SMARTCOS 的版本号
T5	XX	卡片状态字节
T6-T7	8638	明华公司 IC 卡制造机构标识号
T8-TD	XX	卡唯一序号

卡状态字节描述如下：

B7	B6	B5	B4	B3	B2	B1	B0	状态
0	X	X	0	X	X	X	X	该卡已初始化，并成功
1	X	X	0	X	X	X	X	该卡未被初始化
1	X	X	1	X	X	X	X	该卡初始化过程被锁
0	0	0	0	0	0	X	X	该卡未个人化
0	0	1	0	X	X	X	X	该卡个人化未结束
0	1	1	0	X	X	X	X	该卡个人化成功
0	0	0	1	X	X	X	X	该卡个人化没有成功，卡被锁
0	1	1	1	X	X	X	X	该卡个人化成功，卡被锁

5、 基本命令集

5.1、 命令与应答机制

智能卡与接口设备之间使用命令与应答的通信机制，即接口设备发送命令，智能卡接收并处理后发送响应给接口设备。这种机制包括两种数据单元——命令应用数据单元与响应应用数据单元。

命令应用数据单元包含两部分：固定的四个字节命令头和长度可变的命令体，其内容参见如下表格：

命 令 头				命 令 体		
CLA	INS	P1	P2	Lc	数据域	Le

CLA 字节指出命令的类型。如下表所述：

B7	B6	B5	B4	B3	B2	B1	B0	定 义
1 0								外部命令 内部命令
				1 0				安全报文传送 不附加安全报文件传送

INS 字节表示命令编码，P1 和 P2 为具体命令参数。

Lc 字节表示命令报文数据域的长度，只有一个字节表示，取值范围为 1-110。如果 Lc 为 0 表示没有数据域。

Le 表示期望卡返回的数据长度，由单字节表示，取值范围 1-110。

响应报文数据域也包括两部分：可能存在的响应数据体（应答体）和两个状态字节（应答尾部），如下表所示：

应答体	应答尾部	
响应数据体	SW1	SW2

5.2、 命令与应答编码

下面表格显示了命令的编码：

命令	指令类别	编码	用途	兼容性
Create File	80	E0	建立文件	Δ
Write KEY	80/84	D4	增加或修改密钥	Δ
Read Binary	00	B0	读二进制	√*
Update Binary	00/04	D6	修改二进制	√*
Read Record	00	B2	读记录	√*
Update Record	00/04	DC	修改记录	√*
Select File	00	A4	选择文件	√*
Credit For Load	B0	2A	医疗帐户划入	√
Debit For Purchase	B0	2C	医疗消费	√
Get Balance	B0	26	读个人帐户余额	√
Get Transaction Prove	B0	2E	取交易认证	√
Initialize For Load	B0	28	帐户划入初始化	√
Initialize For Purchase	B0	28	医疗消费初始化	√
Update Starting Day	B0	56	修改起始日期	√
Application Block	84	1E	应用锁定	√
Card Block	84	16	卡片锁定	√
External authentication	00	82	外部认证	√*
Get Challenge	00	84	产生随机数	√*
Get Response	00	C0	取响应	√*
Internal Authentication	00	88	内部认证	√*
Verify	00	20	校验 PIN	√*
Change PIN	80	5E	修改 PIN	√
Pin Change/Unblock	84	24	重装/解锁 PIN	√
Crypt	80	F6	安全模块指令	Δ
Generate KEY	80	FA	生成过程密钥	Δ

√ 表示遵照《社会保障（个人）卡规范》

* 表示遵照 ISO/IEC 7816-4。

Δ 表示为自定义指令。

下表列出了一部分不针对具体命令的应答尾部状态字节（SW1、SW2）的编码定义，在以后对具体命令的描述中再列出与各个命令相关的状态字节。

正常返回码：

状态码	含义说明
90 00	正常结束

61　XX	正常结束，仍有 XX 个有效数据可取

错误或警告返回码

状态码	含义说明
63 CX	剩余尝试次数
65　81	写 EEPROM 失败
67　00	数据长度错误
69　01	无效的状态
69　81	文件类型不匹配
69　82	安全状态不满足
69　83	密钥已经被锁住
69　85	使用条件不满足
69　88	安全报文数据项不正确
6A　80	数据域参数不正确
6A　81	功能不支持
6A　82	没有找到文件
6A　83	没有找到记录
6A　84	没有足够的空间
6A　86	P1，P2 参数不正确
6A　88	密钥未找到
6B　00	参数错误（偏移地址超出了 EF 文件长度）
6D　00	不正确的 INS
6E　00	不正确的 CLA
6F　00	未定义的错误
93　02	MAC 无效
93　03	应用永久锁定
94　01	金额不足
94　03	密钥索引不支持
94　06	所需 MAC 不可用

6、 命令描述

本章将对集中对每条命令的功能、使用条件、命令格式及其参数、响应格式及其参数做详细的描述，其中各命令参数及响应参数的编码均为十六进制。

6.1、 Create File 建立文件

1）.定义和范围

Create File 命令用于建立 MF 文件、DF 文件和 EF 文件。

当建立 MF 文件时，卡片必须为空，卡片首先验证制造商密钥，通过后把主控文件（MF）的数据写入 EEPROM。

建立 DF 文件时，只有 MF 存在且有足够的空间，并且满足当前建立文件的安全条件，MF 没有被锁住，才可建立 DF。

建立 EF 文件时，只有卡空间>EF 文件头+文件体，并且满足当前建立 EF 文件的安全条件才可建立 EF。

2）.命令报文

代码	值
CLA	80
INS	E0
P1	00-- 建立 MF 01-- 建立 DF 02-- 建立 EF
P2	00-- 正在建立 01-- 建立结束（MF、DF）
Lc	文件信息长度
DATA	文件信息

3）.命令报文数据域

文件信息及其长度在建立不同类型的文件分别描述如下：

① 建立 **MF** 文件时数据域的信息

Lc	有关文件信息

0F/1A	传输代码 (8 字节)	建立文件权限 (1 字节)	短文件标识符 (1 字节)	MF 的名称 (05-10 字节)

8 个字节的传输代码是由工厂在卡片制造时设定的，如用户无特殊要求，则为：FF FF FF FF FF FF FF FF，在建立 MF 时，若传输代码错误，则内部错误计数器加一，超过 4 次卡片自动锁死不可再用。

短文件标识符指明 MF 下的应用列表文件，该文件是一个变长的记录文件，有效表示为该字节的高三位为 000，低 5 位为短文件的标识符。无列表文件填 00。

如果建立社保应用，则 MF 必须取名为：SX1.SH.SSSE。

② 建立 DF 文件时数据域的信息

Lc	有关文件信息			
09/14	文件标识符 (2 字节)	建立文件权限 (1 字节)	00	DF 的名称 (05-10 字节)

③ 建立 EF 文件时数据域的信息

Lc	有关文件信息						
08	文件标识符 FID (2 字节)	短文件标识符 SFI (1 字节)	文件类型 (1 字节)	权限 1 (1 字节)	权限 2 (1 字节)	Len1 (1 字节)	Len2 (1 字节)

文件类型说明见下表：

文件类型								类型描述
B7	B6	B5	B4	B3	B2	B1	B0	状态
				0	0	0	0	二进制
				0	0	0	1	定长记录
				0	0	1	0	变长定长
				0	0	1	1	循环记录
				0	1	0	0	ATR 文件
				0	1	0	1	密钥文件
				0	1	1	0	医疗保险个人帐户文件
0	0							数据以明文形式写入
0	1							数据以明文+MAC 形式写入
1	0							数据以密文形式写入
1	1							数据以密文+MAC 形式写入
其他值								系统保留

短文件标识符 SFI 说明见下表：

B7	B6	B5	B4	B3	B2	B1	B0	状态
X	X	X	—	—	—	—	—	具体编码见 SFI 高三位说明
—	—	—	X	X	X	X	X	短文件标识符 SFI（取值范围'01'~'1E'）
—	—	—	0	0	0	0	0	所建的 EF 不需要短文件标识符 SFI
—	—	—	1	1	1	1	1	系统保留

短文件标识符 SFI 高三位编码说明：

B7	B6	B5	状态说明
0		0	文件的读控制由权限 1 给定
1		1	文件的读控制由权限 1 与 PIN 共同给定（即两个安全条件为与的关系）
1		0	文件的读控制由权限 1 或由 PIN 给定（即两个安全条件为或的关系）
	0	0	文件的写控制由权限 2 给定
	1	1	文件的写控制由权限 2 与 PIN 共同给定（即两个安全条件为与的关系）
	1	0	文件的写控制由权限 2 或由 PIN 给定（即两个安全条件为或的关系）
其他值			系统保留

权限 1、权限 2 说明如下：

① 对于基本工作文件，权限 1 指明读权限，权限 2 指明更新权限；

② 对于密钥文件，权限 1 指明增加新密钥的权限，权限 2 系统保留，建议添 00H。

③ 钱包文件、存折文件的权限 1、权限 2 由系统保留。

Len1 、Len2 说明如下：

① 对于二进制文件、变长记录文件，Len1 和 Len2 两字节表示文件长度。文件长度应大于 00H,小于等于 7FFFH。

② 对于 ATR 文件，Len1 和 Len2 两字节表示文件长度。文件长度应大于 00H,小于等于 0008H。

③ 对于定长记录文件、循环定长记录文件，Len1 指明记录数，Len2 指明记录长度。Len1 不能为零，Len2 不能超过 110 个字节。

④ 对于密钥文件，Len1 指明记录数，Len2 系统保留。

⑤ 对于医疗保险个人帐户文件，Len1，Len2 均为系统保留。

⑥ 需特殊指明，如果用户要建立 ATR 文件，则无法获得该卡的唯一序列号。

⑦ 对以上系统保留的字节，建议用户填写 00。

4）.特殊说明

建立 MF、DF 文件分别对应着 Create End 命令，当 Create End 成功执行之后，文件的安全条件才会有效。在执行此命令之前 SmartCOS 一直处在个人化状态，即使卡重新复位，SmartCOS 也能继续上次的个人化过程，直到收到 Create End 指令。其格式分别为：

CreateEnd DF

代码	值
CLA	80
INS	E0
P1	01
P2	01
Lc	02
DATA	FID

CreateEnd MF

代码	值
CLA	80
INS	E0
P1	00
P2	01
Lc	02
DATA	3F 00

5）.响应报文数据域

响应报文数据域不存在。

6）.响应报文状态码

SW1 SW2	**意义**
90　00	命令正确执行
65　81	写 EEPROM 失败
67　00	数据长度错误
63　CX	允许传输代码错误次数

69　01	创建状态不满足
69　82	安全条件不满足
6A　80	标识符已存在
6A　81	功能不支持（文件不可建立在 MF 或 DF）
6A　82	文件未找到
6A　84	没有足够的空间
6A　86	P1 或 P2 参数不正确
6D　00	不正确的 INS
6E　00	不正确的 CLA
93　03	应用永久锁定

附加说明：

特殊的文件标识符：

"EF 08"在社保 SmartCOS 中用作交易明细文件的标识符，"08"是该文件的短文件标识符，该文件是一个循环定长记录文件，用来记录每一个交易的相关数据。

《社会保障（个人）卡规范》规定社保交易明细文件支持两种记录长度：

① 当交易明细文件的记录长度为 14H 字节时，表示仅支持个人帐户医疗 消费处理模式；

② 当交易明细文件的记录长度为 1CH 时，表示支持个人帐户、个人自付、统筹基金支付三种医疗消费处理模式。

建立医疗个人帐户文件后必须建立一个交易明细文件用来记录每一笔交易，如果没有该文件则交易将无法完成。

6.2、 Write KEY 增加或修改密钥

1）.定义和范围

WRITE KEY 命令可向卡中装载或更新卡中已经存在的密钥。本命令可支持 8 字节或 16 字节的密钥（个人 PIN 除外）。密钥写入可以是明文或密文的方式。当本命令用于增加密钥时必须满足密钥文件的修改权限。在需要以明文加 MAC 方式或以密文加 MAC 方式安装/修改 KEY 之前，必须用 GET CHANLLEGE 命令从 IC 卡中取一个 4 字节的随机数。

社保 SmartCOS 规定，密钥标识为”0”，密钥版本为”0”的外部认证密钥为主控密钥。

2）.命令报文

明文安装或修改 KEY 的命令报文如下：

代码	值
CLA	80
INS	D4
P1	00 -- 安装密钥 01 -- 修改密钥
P2	00
Lc	密钥信息长度
DATA	密钥信息

密文安装或修改 KEY 的命令报文如下：

代码	值
CLA	84
INS	D4
P1	00 -- 安装密钥 XX -- 密钥类型 （用于修改密钥）
P2	00 -- 安装密钥 XX -- 密钥标识（用于修改密钥）
Lc	数据长度
DATA	密钥信息

注：当密钥类型和标识都为 00 时，如果密钥文件为空，则表示安装卡片（或

应用）的主控密钥。

3）.命令报文数据域

①．明文形式的数据域信息

其中密钥信息如下：

密钥信息（8 个字节密钥头+密钥值）									
密钥头									密钥值
密钥标识(1)	版本号(1)	算法标识(1)	密钥类型(1)	使用权限(1)	后续状态(1)	修改权限(1)	初始错误计数(1/2)	当前错误计数(1/2)	空（针对个人PIN）；(02-10)

[注]：

密钥标识符（KID）： 不能等于 00h 和 FFh，同类型密钥的标识符必须唯一。

版本号： 同类密钥的版本。

算法标识：算法标识缺省为 00，算法是 Triple DES，如果是 Single DES 则算法标识为 01，算法标识对 PIN 没有意义。如果用户在 SmartCOS-PSAM 中定义了自己的算法，此处必须指明算法为 08。对于其它值系统保留。

使用权限：指使用某一密钥时所需满足的安全条件。

修改权限：指用 Write KEY 指令修改某一密钥时所需满足的安全条件。

后续状态：只对 PIN、和外部认证 KEY 有效。当口令核对成功或外部认证成功后，置卡片状态机为后续状态的低半字节。

错误计数器：错误计数器的高半字节为初始错误计数，指明密钥可以连续错误的最多次数；错误计数器的低半字节为当前错误计数，指明当前还可允许的错误次数。如果连续错误的次数超过初始错误计数的值，密钥自动锁死。

SmartCOS 支持的密钥类型如下表所列：

KEY 类型	该类型 KEY 作用描述
00	消费取现密钥
01	帐户划入密钥

02	TAC 密钥
05	应用维护密钥，用于产生应用锁定、应用解锁、卡片锁定和读、更新二进制、记录命令的 MAC
08	外部认证密钥，用于外部认证过程
09	内部认证密钥，用于内部认证过程
0B	个人密码（PIN），用于个人密码校验
0C	超级密码
其它	系统保留

说明：

每一个应用下只能有一个个人密码（PIN），PIN 的长度为 2～8 个字节，内容必须为 0～9 的数字。超级 PIN 在每一个目录下也唯一，长度为 2～8 字节，其余密钥的长度为 8 或 16 个字节。

②．明文+MAC 形式的数据域信息

明文密钥信息	**4 字节 MAC**

本条命令中 MAC 不采用过程密钥方式而是用主控密钥直接对以下数据进行 MAC 计算（按所列顺序）产生的：

——CLA

——INS

——P1

——P2

——Lc

——密钥标识

——密钥版本号

——算法标识

——密钥类型

——使用权限

——后续状态

——修改权限

——错误计数器

——密钥值

加密和 MAC 计算的方法遵循《社会保障（个人）卡规范》。生成 MAC 码

的初始值为：4 个字节的随机数+00 00 00 00。

③．密文形式的数据域信息

加密后的密钥信息

密文形式的数据域信息：

密钥密文信息使用主控密钥直接（无须产生过程密钥）对以下数据加密（按所列顺序）产生的：

——密钥标识

——密钥版本号

——算法标识

——密钥类型

——使用权限

——后续状态

——修改权限

——错误计数器

——密钥值

④．密文加 MAC 形式的数据域信息

加密后的密钥信息	4 字节 MAC

命令数据域中的加密后的密钥信息按以下方法获得：

使用主控密钥直接（无须产生过程密钥）对以下数据加密（按所列顺序）产生：

——密钥标识

——密钥版本号

——算法标识

——密钥类型

——使用权限

——后续状态

——修改权限

——错误计数器

——密钥值

命令数据域中的 MAC 按以下方法获得：

用主控密钥直接对以下数据进行 MAC 计算（按所列顺序）产生

——CLA

——INS

——P1

——P2

——Lc

——加密后的密钥信息

在 MF 下装载密钥的控制过程为：

——卡片主控密钥在卡片传输密钥的控制下装载。

——卡片主控密钥在卡片主控密钥的控制下更新。

——卡片维护密钥在卡片主控密钥的控制下装载和更新。

在 DF 下装载密钥的控制过程为：

——应用主控密钥在卡片主控密钥的控制下装载。

——应用主控密钥在应用主控密钥的控制下更新。

——应用维护密钥在应用主控密钥的控制下装载和更新。

——应用主工作密钥在应用主控密钥的控制下装载和更新。

SmartCOS 规定：密钥标识为”00”，密钥版本为”00”的外部认证密钥为主控密钥。应用下的其他密钥均由应用主控密钥加密安装。对密钥信息的加密方式按标准的 Triple DES 或 Single DES，请参考 7.4。

MAC 是用主控密钥直接（无须产生过程密钥）对以下数据进行 MAC 计算（按所列顺序）产生的：

——CLA

——INS

——P1

——P2

——Lc

——密钥密文信息

加密和 MAC 计算的方法遵循《社会保障（个人）卡规范》。生成 MAC 码的初始值为：4 个字节的随机数+00 00 00 00。

密文安装应用主控密钥时，所使用的密钥为上一层的卡片主控密钥。

密文安装 MF 下的卡片主控密钥时，则使用卡片的传输密钥进行安装。

[注]：无论明文密文，在修改密钥时，均不能改动密钥标识符和密钥类型。

3）.响应报文数据域

响应报文数据域不存在。

6）.响应报文状态码

SW1 SW2	意义
90 00	命令正确执行
65 81	写 EEPROM 失败
67 00	数据长度错误
69 01	功能不支持
69 81	命令与文件类型不相符
69 82	安全条件不满足
69 83	密钥锁定
69 84	取随机数无效
69 85	使用条件不满足（应用被锁定）
69 88	MAC 码不正确
6A 80	数据域不正确
6A 81	卡片锁定
6A 82	文件未找到
6A 84	文件空间不够
6A 86	P1、P2 不正确
6D 00	不正确的 INS
6E 00	不正确的 CLA
93 03	应用永久锁定
94 03	没有找到 KEY

6.3、 Generate KEY 生成子密钥或过程密钥

1）.定义和范围

Generate KEY 命令使用 SAM 主密钥或外部认证主密钥生成子密钥或过程密钥存放在 RAM 中以供后续命令使用。

2）.命令报文

代码	值
CLA	80
INS	FA
P1	00- 生成子密钥 生成过程密钥（长度必须为 10H）
P2	SAM 或外部认证主密钥标识符
Lc	08/10
DATA	用户数据

3）.命令报文数据域

用于生成子密钥的主密钥必须是 SAM 主密钥或外部认证主密钥,否则将返回密钥不存在 9403。

过程密钥存在卡的 RAM 中，下电、复位或生成过程密钥后自动丢失。其生成过程如下：

首先用加密密钥对输入数据的左8个字节进行加密生成子密钥的左半部分；

然后用加密密钥对输入数据的左 8 个字节求反后进行加密生成子密钥的右半部分。

最后用刚生成的子密钥作为密钥对输入数据的右 8 个字节进行 Triple DES 加密，加密的结果即为过程密钥。

按银行规范，左 8 个字节为应用序列号，右 8 个字节是当次交易的部分数据，由于每张卡的应用序列号唯一性和交易数据的随机性，所以生成的过程密钥也具有唯一性。生成过程密钥的过程完全在卡的内部完成，与外界无关，从而提高了系统的安全性。

子密钥的生成同过程密钥的前两步，因此输入的数据只有 8 个字节。

4）.响应报文数据域

响应报文数据域不存在。

5）.响应报文状态码

SW1 SW2	意义
90 00	命令正确执行
67 00	Lc 不是 16 个字节
69 83	密钥已经锁定
69 82	不满足安全状态
6A 81	功能不支持
6A 82	文件未找到
93 03	应用永久锁定
94 03	密钥未找到

6.4、 Crypt 安全模块命令

1）.定义和范围

该指令使用卡中已经存在的密钥对数据进行加密、解密、生成交易 MAC 码或应用 MAC 码。

2）.命令报文

Crypt 的命令报文如下：

代码	值
CLA	80
INS	F8
P1	00--加密数据 01--解密数据 02--生成交易 MAC 码 03--生成应用 MAC 码
P2	00 或指定密钥的标识符
Lc	Lc
DATA	用户数据
Le	期望返回数据长度

3）.命令报文数据域

P2≠00 且 P1=00、01、02、03 时，P2 指定的密钥如果不是 P1 指定的加密类型密钥，将返回 9403；如果 P2=00，则使用子密钥进行加、解密、MAC 码生成。

DES 加、解密的输入数据长度不超过 48 个字节，方法同本手册的 7.4 节。生成交易 MAC 的数据可以不是 8 的倍数，方法同本手册的 7.3，只是生成 MAC 的初始值为 8 个 00。当生成应用 MAC 时，数据长度必须大于 8 且数据域前 8 个字节为初始值，之后的数据为生成 MAC 的数据。

DES 加、解密及生成 MAC 码的运算方法请参见《社会保障（个人）卡规范》的运算方法。

4）.响应报文数据域

响应报文数据域为加密后的数据。

5）.响应报文状态码

SW1 SW2	意义
90　00	命令正确执行
61　XX	正常执行，但仍有 XX 个数据有效待取
67　00	错误的长度
69　81	P2 指定的密钥不是 Crypt 密钥
69　82	不满足安全状态
6A　81	功能不支持
94　03	密钥未找到

6.5、 Application Block 应用锁定

1）.定义和范围

Application Block 命令使当前选择的应用失效。

当 Application Block 成功完成后，用 Select File 命令选择已失效的应用，将回送状态“选择文件无效”(状态码 SW1 SW2=‘6A81’)。

对其它命令的影响根据不同的应用而定。

2）.命令报文

代码	值
CLA	84
INS	1E
P1	00
P2	00- 临时锁定应用 01- 永久锁定应用
Lc	04
DATA	4 字节的报文鉴别代码(MAC)数据元，由应用维护密钥生成。
Le	不存在

3）.命令报文数据域

对于临时锁定的应用可以用 Application Unblock 命令解锁，可由 Select File 命令选择进入该目录，但对文件操作时返回‘6A81’。对于永久锁定的应用，社保 SmartCOS-社保 V1.5 将不允许执行 Application Unblock 命令，可用 Select File 命令选择进入该目录，但对文件操作时返回‘6983’。

4）.响应报文数据域

响应报文数据域不存在。

5）.响应报文状态码

SW1 SW2	意义
90 00	命令正确执行
65 81	内存失败

69　82	安全状态不满足
69　88	安全报文数据项不正确
6A　86	参数 P1 P2 不正确
94　03	未找到引用数据

6.6、 Application Unblock 应用解锁

1）.定义和范围

Application Unblock 命令用于恢复当前应用。如果某应用连续三次解锁失败，则社保 SmartCOS V1.5 将永久锁定此应用。

2）.命令报文

代码	值
CLA	84
INS	18
P1	00
P2	00
Lc	04
Data	4 个字节的报文鉴别代码(MAC)数据元，使用应用维护密钥生成。

3）.命令报文数据域

命令报文数据域为 4 个字节的报文鉴别代码(MAC)数据元，使用应用维护密钥生成。

4）.响应报文数据域

响应报文数据域不存在。

5）.响应报文状态码

SW1	SW2	意义
90	00	命令正确执行
65	81	写 EEPROM 不成功
69	82	不满足安全状态
69	85	使用条件不满足
69	88	安全报文数据项不正确
93	03	应用永久锁定

6.7、 Card Block 卡片锁定

1）.定义和范围

Card Block 命令使卡中所有应用永久失效。

当 Card Block 命令成功完成后。所有后续的命令都将回送状态码‘6A81’（不支持此功能），且不执行任何其它操作。

2）.命令报文

代码	值
CLA	84
INS	16
P1	00
P2	00
Lc	04
DATA	4 个字节的报文鉴别代码(MAC)数据元，使用应用维护密钥生成。

3）.命令报文数据域

命令报文数据域为 4 个字节的报文鉴别代码(MAC)数据元，使用应用维护密钥生成。

4）.响应报文数据域

响应报文数据域不存在。

5）.响应报文状态码

SW1 SW2	意义
90 00	命令正确执行
65 81	内存失败
69 82	不满足安全状态
69 88	安全报文数据项不正确

6.8、 External Authentication 外部认证

1）.定义和范围

External Authentication 命令用于对卡片外部的安全认证，过程如下：首先执行产生随机数命令，从卡中直接获取 8 字节的随机数或 4 字节的随机数并补 00 00 00 00 后，在卡片外部用已知密钥加密。对卡片执行外部认证命令，数据域为用上述方法得到的加密数据。IC 卡将命令中的数据域用指定的外部认证密钥解密，然后与先前产生的随机数进行比较。如果一致，则表示认证通过，置安全状态寄存器为该密钥规定的后续状态值，错误允许计数器恢复成初始值；如果不一致，则认证失败，错误允许计数器值减 1，且不改变安全状态寄存器的值。

2）.命令报文

代码	值
CLA	00
INS	82
P1	00
P2	00 或密钥标识符
Lc	8
DATA	加密后的随机数

3）.命令报文数据域

- 命令报文数据域中包含 8 字节的加密数据，该数据是用主控密钥对此命令前一条命令“ GET CHALLENGE ”命令获得的随机数后缀“ 00 00 00 00 ”之后做 3DES 加密运算。若校验成功，则安全状态寄存器的值被置成该密钥的后续状态，同时错误允许计数器被置成初始值。若校验错误，则再试次数减 1。若外部认证密钥已被锁死，则不能再执行该命令。被锁死后的外部认证密钥不能再恢复。
- 如果存在全局外部认证 KEY，则其后续状态与全局外部认证 KEY 的后续状态进行或操作组成全局后续状态。
- 若校验失败时，IC 卡将回送 SW1 SW2＝63CX，X 表示允许重试的次数。当卡回送 63C0 时，表示不能重试，此时再使用校验命令时，将回送失败状态

码‘6983’，密钥将被锁。

4）.响应报文数据域

响应报文数据域不存在。

5）.响应报文状态码

SW1 SW2	意义
90 00	命令正确执行
63 CX	校验失败，X 表示允许重试的次数
65 81	写 EEPROM 失败
67 00	长度错误
69 81	当前文件不是线性定长文件或线性变长文件
69 82	写的条件不满足
69 83	密钥已经锁定
69 84	随机数无效
69 85	应用临时锁定
69 88	MAC 不正确
6A 81	不支持此功能(无 MF 或 MF 已锁定)
6A 82	未找到文件
6A 83	未找到记录
6A 84	文件中存储空间不够
6A 86	P1 或 P2 不正确
6D 00	不正确的 INS
6E 00	不正确的 CLASS
93 02	应用永久锁定
93 03	密钥索引不支持

6.9、 Get Challenge 产生随机数

1）.定义和范围

Get Challenge 命令请求一个用于外部认证过程或其它过程的随机数。

使用卡内随机数的前一条命令必须是 Get Challenge 命令。卡产生 Le 字节的随机数送给终端。若下一条指令为外部认证，则卡将从外部传入的外部认证数据用指定的外部认证密钥解密后与该随机数进行比较。

2）.命令报文

代码	值
CLA	00
INS	84
P1	00
P2	00
Le	04/08/10

3）.命令报文数据域

命令报文数据域不存在。

4）.响应报文数据域

取长度为 4 的随机数后，卡内随机数为 4 个随机数+00 00 00 00。

5）.响应报文状态码

SW1 SW2	意义
90 00	命令正确执行
67 00	长度错误
6A 86	参数 P1 P2 不正确

6.10、 Get Response 取响应

1）.定义和范围

Get Response 命令提供了一种从卡片向接口设备传送 APDU （或 APDU 一部分）的传输方法。

2）.命令报文

代码	值
CLA	00
INS	C0
P1	00
P2	00
Le	应答的期望数据长度

3）.命令报文数据域

命令报文数据域不存在。

4）.响应报文数据域

期望应答的数据。

5）.响应报文状态码

SW1 SW2	意义
90　00	命令正确执行
61　XX	还有 XX 数据可返回
67　00	长度错误(Lc 大于卡中应答数据长度)
6C　XX	长度错误（Le 不正确，‘XX’表示实际长度）
6F　00	卡中无数据返回

6.11、 Internal Authentication 内部认证

1）.定义和范围

Internal Authentication 命令提供了利用接口设备发来的随机数和自身存储的相关密钥进行数据认证的功能。过程如下：在卡的外部产生 8 个字节的随机数后，卡片执行内部认证命令，数据域为上述方法产生的随机数。IC 卡将命令中的数据域用指定的内部认证密钥加密后送出卡外。

2）.命令报文

代码	值
CLA	00
INS	88
P1	00
P2	00 或密钥标识符
Lc	08
DATA	认证数据

3）.命令报文数据域

命令报文数据域 DATA 的内容是应用专用的认证数据。

4）.响应报文数据域

应答报文数据域是相关认证数据 DES 运算的结果。

5）.响应报文状态码

SW1 SW2	意义
90　00	命令正确执行
67　00	长度 Lc 不正确
69　01	状态无效
69　82	不满足安全条件
69　85	使用条件不满足
6A　82	ISF 文件未找到
94　03	密钥未找到

6.12、 PIN Change/Unblock 个人密码的解锁

1）.定义和范围

PIN Change/Unblock 命令给发卡方提供了解锁个人密码或更改个人密码的功能。命令中个人密码的传递采用加密方式。

2）.命令报文

代码	值
CLA	84
INS	24
P1	00
P2	00--解锁个人密码。仅重置尝试计数器，并不更改个人密码。 01--更改个人密码。重置尝试计数器并以新 PIN 取代旧 PIN。
Lc	04 -- P2=00 0C/14 -- P2=01
DATA	加密的个人密码数据元和报文鉴别代码（MAC）数据元
Le	不存在

3）.命令报文数据域

解锁个人密码：Lc=04，包括 MAC 数据元，解锁成功后应重置错误计数器，不改变个人密码。

更改个人密码：Lc=0C/14，包括被加密的个人密码数据元和 MAC 数据元。

解锁/更改个人密码，采用的密钥为应用维护密钥对随机数加密产生的过程密钥。

4）.响应报文数据域

响应报文数据域不存在。

5）.响应报文状态码

SW1 SW2	意义
90 00	命令正确执行
63 CX	X 表示允许重试的次数
65 81	写 EEPROM 失败
69 82	不满足安全状态
69 85	使用条件不满足

69　88	安全报文数据项不正确
6A　80	数据不正确
6A　82	未找到 ISF 文件
6A　86	参数 P1 P2 不正确
94　03	密钥未找到
93　03	应用永久锁定

6.13、 Read Binary 读二进制

1）.定义和范围

Read Binary 命令用于读取二进制文件的内容。

2）.命令报文

代码	值
CLA	00
INS	B0
P1	XX
P2	XX
Le	XX

若 P1 的高三位为 100，则低五位为短的文件标识符，P2 为欲读内容首字节的偏移量。若 P1 的最高位不为 1，则 P1 P2 为欲读内容首字节的偏移量，所读文件为当前文件。

Le 表示要读取的字节数，最大值为 110。若 Le 为 00 ，则送回警告状态 6C XX，请求 Le 置为 XX 并重发该命令。

3）.命令报文数据域

命令报文数据域不存在。

4）.响应报文数据域

应答报文数据域的内容为读出的二进制文件的内容。

5）.响应报文状态码

SW1 SW2	意义
90 00	命令执行错误
69 81	不是二进制文件
69 82	不满足安全条件
6A 81	不支持此功能
6A 82	未找到文件
6B 00	参数错误(偏移地址超出了 EF)
6C XX	长度错误（Le 不正确，‘ XX ’表示实际长度）

6.14、 Read Record 读记录

1）.定义和范围

Read Record 命令用于读取记录文件的内容。该命令适用于定长记录文件、循环定长记录文件、变长记录文件。

2）.命令报文

代码	值
CLA	00
INS	B2
P1	记录号或记录标识符
P2	引用控制参数
Le	00 或要读出的数据的长度

记录号的取值范围为‘01’-‘FE’，‘00’表示当前记录。

下表定义了命令报文中的引用控制参数。

B7	B6	B5	B4	B3	B2	B1	B0	含义
0	0	0	0	0				对当前文件进行操作
x	x	x	x	x				基本文件标识符
					1	0	0	读 P1 指定的记录
					1	0	1	从 P1 指定的记录开始读到最后一个记录
					1	1	0	从最后一个记录读到 P1 指定的记录
					0	0	0	读第一个具有 P1 指定的记录标识符的实例
					0	0	1	读最后一个具有 P1 指定的记录标识符的实例
					0	1	0	读下一个具有 P1 指定的记录标识符的实例
					0	1	1	读上一个具有 P1 指定的记录标识符的实例

3）.命令报文数据域

命令报文数据域不存在。

4）.响应报文数据域

响应报文数据域由读取的记录组成。

5）.响应报文状态码

SW1 SW2	意义
90　00	命令正确执行
67　00	长度错误
69　81	文件类型错误
69　85	使用条件不满足
69　82	读条件不满足
69　86	不满足命令执行条件（无当前 EF）
6A　81	不支持此功能
6A　82	未找到文件
6A　83	未找到记录
6A　86	参数 P1、P2 不正确
6C　XX	长度错误（Le 不正确，‘ XX ’ 表示实际长度）
93　03	应用永久锁定

6.15、 Select File 选择文件

1）.定义和范围

Select File 命令通过文件名来选择 IC 卡中的文件。

2）.命令报文

代码	值
CLA	00
INS	A4
P1	00- 按文件标识符选择 MF 或 DF 02- 选择 EF 04- 按文件名选择应用
P2	00- 第一个或仅有的一个 02-下一个
Lc	XX
DATA	文件标识符或 DF（MF）名称

3）.命令报文数据域

命令报文数据域为文件标识符或文件名称。

如果命令报文数据域为空且 P1=00H 时，该命令选择主控文件（MF）。

4）.响应报文数据域

应答报文数据域包括所选择的 DDF 或 ADF 的文件控制信息 FCI,采用 LV 格式。

DDF 回送的文件控制信息 FCI：

标志 L	值（Value）	存在方式
6F	文件控制信息模板	必备
84	DF 名	必备
A5	文件控制信息专用模板	必备
88	目录基本文件的短文件标识符	必备

ADF 回送的文件控制信息 FCI：

标志 L	值（Value）	存在方式
6F	文件控制信息模板	必备
84	DF 名	必备

A5	文件控制信息专用数据	必备
9F 0C	发卡方自定义数据的文件控制信息	可选

EF 回送的文件控制信息 FCI：

标志 L	值（Value）	存在方式
6F	文件控制信息模板	必备
A5	文件控制信息专用数据	必备
9F 0C	EF 文件控制信息（含文件标识符、类型、长度）	必备

5）.响应报文状态码

SW1 SW2	意义
90　00	命令执行正确
61　XX	还有 XX 个数据需要取回
67　00	数据长度错误
6A　81	不支持此功能(无 MF 或应用已锁)
6A　82	未找到文件
6A　86	参数 P1 P2 不正确

6.16、 Update Binary 修改二进制

1）.定义和范围

Update Binary 命令用于以密文或明文的形式修改二进制文件。

2）.命令报文

代码	值
CLA	00/04
INS	D6
P1	XX
P2	XX
Lc	XX
DATA	写入的数据

参数说明： 若 P1 的高三位为 100，则低五位为二进制文件的短文件标识符，P2 为欲写内容首字节的偏移量。若 P1 的最高位不为 1，则 P1 P2 为欲读内容首字节的偏移量，所写文件为当前文件。

说明如下：

B7	B6	B5	B4	B3	B2	B1	B0	指令状态
1								使用 SFI 方式
	0	0						RFU（如果 b8=1）
			X	X	X	X	X	SFI

3）.命令报文数据域

命令报文数据域包括更新原有数据的新数据。使用安全报文时，命令中的数据域包明文+MAC 或者密文+MAC。MAC 是由卡片维护密钥或应用维护密钥对更新原有数据的新数据进行计算而得到的。

- 当文件类型最高位为 0，次高位也为 0 时采用明文形式，Lc 表示要写入的字节数，DATA 为要写入的数据。
- 当文件类型最高位为 1，次高位为 0 时采用明文+MAC 安全报文形式，Lc 为要写入的字节数 + 4 字节安全报文，DATA 为要写入的明文数据 + 4 字节安全报文。
- 文件类型的最高位为 0，次高位为 1 时采用密文形式。写二进制文件时，

若 CLA 与文件类型的第 4 位不匹配，如 CLA 为 04，而文件类型为 00 时，则返回“ 6A 81 ”。

- 当文件类型最高位为 1，次高位也为 1 时采用密文+MAC 安全报文形式，Lc 为要写入的字节数 + 4 字节安全报文，DATA 为要写入的密文数据 + 4 字节安全报文。其中生成密文数据的明文形式为：明文数据长度（Len）+明文数据+补位（00）
- 数据域长度的最大值为 110 个字节。

注：二进制文件类型为 00 时，数据也可以以密文+MAC 形式写入。

4）.响应报文数据域

响应报文数据域不存在。

5）.响应报文状态码

SW1 SW2	意义
90 00	命令正确执行
65 81	写 EEPROM 失败
67 00	长度错误
69 81	不是二进制文件
69 82	写的条件不满足
69 84	没有取随机数
69 88	安全报文数据项不正确
69 85	使用条件不满足（应用临时锁定）
6A 81	不支持此功能(无 MF、应用已锁或 CLA 与文件类型不符)
6A 82	未找到文件
6A 86	P1 或 P2 不正确
6B 00	P1 或 P2 超限
6D 00	不正确的 INS
6E 00	不正确的 CLASS
93 02	应用永久锁定
93 03	密钥索引不支持

6.17、 Update Record 修改记录

1）.定义和范围

Update Record 命令用于修改记录文件。该命令适用于定长记录文件和变长记录文件。

2）.命令报文

代码	值
CLA	00/04
INS	DC
P1	= 00 当前记录 ≠00 指定的记录号
P2	XX
Lc	后续数据域的长度
DATA	更新原有记录的新记录

参数说明： P2 的低 3 位为 100，如果高 5 位不为 00000 则表示短文件标识符，否则表示当前文件。本命令可操作的三种记录文件被选择后当前记录都是第一条记录。

说明如下：

B7	B6	B5	B4	B3	B2	B1	B0	指令状态
X	X	X	X	X				使用 SFI 方式
					1	0	0	记录号在 P1 中给出
其余值								保留

3）.命令报文数据域

命令报文数据域由更新原有记录的新记录组成，使用安全报文时，命令中的数据域包括明文+MAC 或者密文+MAC。MAC 是由卡片维护密钥对更新原有记录计算而得到的。

- 命令报文数据域由写入的新记录组成。
- 当文件类型最高位为 0，次高位也为 0 时采用明文形式，Lc 表示要写入的字节数，DATA 为要写入的数据。
- 当文件类型最高位为 1，次高位为 0 时采用明文+MAC 安全报文形式，

Lc 为要写入的字节数 ＋4 字节安全报文，DATA 为要写入的明文数据 ＋4 字节安全报文。

- 文件类型的最高位为 0，次高位为 1 时采用密文形式。写记录文件时，若 CLA 与文件类型的第 4 位不匹配，如 CLA 为 04，而文件类型为 00 时，则返回“ 6A 81 ”。
- 当文件类型最高位为 1，次高位为 1 时采用密文+MAC 安全报文形式，Lc 为要写入的字节数 ＋4 字节安全报文，DATA 为要写入的密文数据 ＋4 字节安全报文。其中生成密文数据的明文形式为 :明文数据长度（Len）+明文数据+补位（00）

4）.响应报文数据域

响应报文数据域不存在。

5）.响应报文状态码

SW1 SW2	意义
90　00	命令正确执行
65　81	写 EEPROM 失败
67　00	长度错误
69　81	当前文件不是线性定长文件或线性变长文件
69　82	写的条件不满足
69　84	随机数无效
69　85	应用临时锁定
69　88	MAC 不正确
6A　81	不支持此功能(无 MF 或 MF 已锁定)
6A　82	未找到文件
6A　83	未找到记录
6A　84	文件中存储空间不够
6A　86	P1 或 P2 不正确
6D　00	不正确的 INS
6E　00	不正确的 CLASS
93　02	应用永久锁定
93　03	密钥索引不支持

6.18、 Verify 校验

1）.定义和范围

Verify 命令用于校验命令数据域个人密码的正确性。

2）.命令报文

代码	值
CLA	00
INS	20
P1	00
P2	00 或密钥标识符
Lc	00 或 02~08
DATA	外部输入的个人密码

当 P2 为 00 时，该命令将自动使用 KID=01 的个人密码。

3）.命令报文数据域

命令报文数据域由持卡者输入的个人密码组成。

- 若校验成功，安全状态寄存器的值被置成该密钥的后续状态，同时错误允许计数器被置成初始值。若校验错误，则可试次数减 1。若个人密码已被锁死，则不能再执行该命令。被锁死的个人密码可以用解锁、重装指令恢复。
- 如果为全局 PIN，则 PIN 为全局后续状态且与其它非全局后续状态进行“或”操作；如果存在全局外部认证 KEY，则其后续状态与全局外部认证 KEY 进行“或”操作组成全局后续状态。
- 命令数据域中外部输入的个人密码与卡中存放的个人密码校验失败时，IC 卡将回送 SW1 SW2＝63CX，X 表示允许重试的次数。当卡回送 63C0 时，表示不能重试，此时再使用校验命令时，将回送失败状态码‘6983’。

4）.响应报文数据域

响应报文数据域不存在。

5）.响应报文状态码

SW1 SW2	意义
90 00	命令正确执行
63 CX	校验失败，X 表示允许重试的次数
65 81	写 EEPROM 失败
67 00	长度错误
69 81	当前文件不是线性定长文件或线性变长文件
69 82	写的条件不满足
69 83	密钥已经被锁住
69 84	随机数无效
69 85	应用临时锁定
69 88	MAC 不正确
6A 81	不支持此功能(无 MF 或 MF 已锁定)
6A 82	未找到文件
6A 83	未找到记录
6A 84	文件中存储空间不够
6A 86	P1 或 P2 不正确
6D 00	不正确的 INS
6E 00	不正确的 CLASS
93 02	应用永久锁定
93 03	密钥索引不支持

6.19、 Change PIN 修改

1）.定义和范围

Change PIN 允许持卡人将指定的个人密码修改为新的密码。当 Change PIN 命令成功完成后，卡片要进行以下操作：

① PIN 尝试计数器复位至尝试次数上限；

② 将指定的个人密码置为新的个人密码。

此命令中的个人密码（PIN）值以明文方式传送。命令数据域中个人密码（PIN）是以 cn 格式存放的，它不需要整字节的填充，只有最低有效位的低半字节可能需要填充，且填以 ‘ F ’。有效的 PIN 至少是 4 个阿拉伯数字。

2）.命令报文

代码	值
CLA	80
INS	5E
P1	01
P2	00 或密钥标识符
Lc	05-0D 或者 11
DATA	当前的 PIN || ‘FF’ || 新的 PIN

当 P2 为 00 时，该命令将自动使用 KID=01 的个人密码。

3）.命令报文数据域

命令报文数据域为指定的 PIN || ‘FF’ || 新的 PIN

4）.响应报文数据域

响应报文数据域不存在。

5）.响应报文状态码

SW1 SW2	意义
90 00	命令正确执行
63 CX	X 表示允许重试的次数
65 81	写 EEPROM 失败
69 82	不满足安全状态
69 83	验证方法锁定

6A　81	功能不支持(无 MF 或卡片已锁死)
6A　82	未找到文件
94　03	密钥未找到

6.20、 UNBLOCK 解锁口令

1）.定义和范围

UNBLOCK 命令用于解锁被锁定的个人密码。

2）.命令报文

代码	值
CLA	80
INS	1C
P1	00
P2	00 或密钥标识符
Lc	PIN 长度
DATA	2-8 字节超级 PIN‖2-8 字节新 PIN

当 P2 为 00 时，该命令将自动使用 KID=01 的个人密码。

3）.命令报文数据域

数据域为 2-8 字节的超级 PIN‖2-8 字节的新 PIN（超级 PIN 只能为数字）。

只有在满足该解锁口令使用条件，且该解锁口令未被锁死时才能执行该命令。命令不改变安全状态寄存器的值。

若解锁口令核对成功，则新口令值将取代解锁口令指定的原口令（不受更改权限的限制），且将口令错误计数器和解锁口令错误计数器恢复成原始值。

若解锁口令失败，则解锁口令可试次数减一，如果超级 PIN 被锁住，则无法被解锁。

5）.响应报文数据域

响应报文数据域不存在。

6）.响应报文状态码

SW1 SW2	意义
90 00	命令正确执行
65 81	写 EEPROM 失败
67 00	数据长度错误
63 CX	允许传输代码错误次数

90 00	命令执行正确
69 01	创建状态不满足
69 82	安全条件不满足
69 85	使用条件不满足（应用临时被锁定）
6A 80	标识符已存在
6A 81	功能不支持（文件不可建立在 MF 或 DF）
6A 82	文件未找到
6A 86	P1 或 P2 参数不正确
6D 00	不正确的 INS
6E 00	不正确的 CLA
93 03	应用永久锁定

6.21、 Initialize For Load 帐户划入初始化

1）.定义和范围

Initialize For Load 命令用于帐户划入交易的初始化。执行该命令后即选择了帐户划入交易，下一条应执行 Credit For Load 命令。Initialize For Load 命令仅对下一条命令有效。这种交易必须在社保终端上联机进行并要求验证口令。

2）.命令报文

代码	值
CLA	B0
INS	28
P1	00
P2	01
Lc	0B
Data	见下表
Le	10

3）.命令报文数据域

Data 说明	长度(字节)
密钥标识符	1
交易金额	4
终端机编号	6

密钥标识符指定的密钥的类型必须为帐户划入子密钥。

4）.响应报文数据域

说明	长度(字节)
卡内医疗保险个人帐户（CIA）旧余额	4
CIA 划入交易序号	2
密钥版本号	1
算法标识	1
伪随机数	4
MAC1	4

过程密钥由密钥标识符指定的帐户划入子密钥对（4 字节随机数+2 字节 CIA 划入交易序号+80 00）加密生成。

MAC1 由卡中过程密钥对（4 字节 CIA 旧余额+4 字节的交易金额+1 字节交

易类型标识+6 字节终端机编号）加密生成。

交易类型标识如下表：

值	含义
31	帐户划入
32	医疗消费

5）.响应报文状态码

SW1 SW2	意义
90 00	命令正确执行
65 81	写 EEPROM 失败
67 00	长度错误
69 85	使用条件不满足
6A 81	不支持此功能能(无 MF 或卡片已锁定)
6A 86	参数 P1，P2 错误
93 03	应用永久锁定
94 03	密钥索引不支持

如果帐户划入初始化不成功，则交易终止。

6.22、 Credit For Load 帐户划入

1）.定义和范围

当帐户划入初始化成功之后，继续进行帐户划入交易。通过帐户划入交易，持卡人可将其在社保基本医疗保险个人帐户上的资金划入卡内医疗保险个人帐户中。这种交易必须在社保终端上联机进行并要求验证口令。

2）.命令报文

代码	值
CLA	B0
INS	2A
P1	00
P2	00
Lc	0B
DATA	见下表
Le	04

3）.命令报文数据域

说明	长度(字节)
交易日期(主机)	4
交易时间(主机)	3
MAC2	4

MAC2 由过程密钥对（4 字节交易金额＋1 字节交易类型标识＋6 字节终端机编号＋4 字节主机交易日期＋3 字节主机交易时间）数据加密生成。

4）.响应报文数据域

4 个字节的交易验证码 TAC	SW1	SW2

TAC 是用系统定义的 TAC 子密钥直接对(4 字节 CIA 新余额＋2 字节的 CIA 划入交易序号（加 1 前）＋4 字节交易金额＋1 字节交易类型标识＋6 字节终端机编号＋4 字节主机交易日期＋3 字节主机交易时间）数据加密生成。

5）.响应报文状态码

SW1 SW2	意义
90　00	命令正确执行
65　81	写 EEPROM 失败

67　00	长度错误
69　01	命令不接受(无效状态)
69　82	不满足安全状态
69　85	使用条件不满足
6A　81	不支持此功能能(无 MF 或卡片已锁定)
93　02	MAC 无效
93　03	应用永久锁定
94　03	密钥索引不支持

【注】 帐户划入交易完成后，CIA 划入交易序号加 1，交易金额累加到 CIA 的余额上，并且在其交易明细文件中存有如下记录：

说明	长度(字节)
CIA 划入交易序号	2 字节
交易类型标识	1 字节
终端机编号	6 字节
主机交易日期	4 字节
主机交易时间	3 字节
交易金额	4 字节

6.23、 Initialize For Purchase 消费初始化

1）.定义和范围

Initialize For Purchase 命令用于医疗消费交易初始化。执行该命令后即选择了医疗消费交易，下一条应执行 Debit For Purchase 命令。Initialize For Purchase 命令仅对下一条命令有效。

2）.命令报文

代码	值
CLA	B0
INS	28
P1	01
P2	01
Lc	13
Data	见下表
Le	16

3）.命令报文数据域

Data 说明	长度(字节)
密钥标识符	1
个人帐户支付金额	4
个人自付金额	4
统筹基金支付金额	4
终端机编号	6

密钥标识符指明的密钥类型必须为消费子密钥。

4）.响应报文数据域

说明	长度(字节)
卡内医疗保险个人帐户（CIA）旧余额	4
个人自付累计（SPIP）旧余额	4
统筹基金支付累计（SPFP）旧余额	4
支付年度	2
医疗消费交易序号	2
密钥版本号	1
算法标识	1
伪随机数	4

5）.响应报文状态码

SW1 SW2	意义
90 00	命令正确执行
62 83	选择文件无效，文件或密钥校验错误
65 81	写 EEPROM 失败
69 82	不满足安全状态
69 85	使用条件不满足
6A 81	不支持此功能能(无 MF 或卡片已锁定)
6A 82	文件未找到
93 03	应用永久锁定
94 01	金额不足
94 03	密钥索引不支持

如果医疗消费初始化不成功，则交易终止。

6.24、 Debit For Purchase 消费

1）.定义和范围

Debit For Purchase 命令用于医疗消费交易。医疗消费交易允许持卡人使用 CIA 进行医疗消费，并记录个人自付和统筹基金支付累计金额。此交易可以在医疗机构终端(POS)上脱网进行。使用 CIA 进行医疗消费交易必须验证口令(PIN)。

2）.命令报文

代码	值
CLA	B0
INS	2C
P1	01
P2	00
Lc	0F
DATA	见下表
Le	08

3）.命令报文数据域

说明	长度(字节)
终端交易序号	4
终端交易日期	4
终端交易时间	3
MAC1	4

过程密钥由密钥标识符指定的消费子密钥对（4 字节随机数+2 字节医疗消费交易序号+终端交易序号的最右 2 个字节）加密生成。

MAC1 由卡中过程密钥对（4 字节的个人帐户交易金额+ 4 字节的个人自付金额+ 4 字节的统筹基金支付金额+1 字节交易类型标识+6 字节终端机编号+3 字节终端交易时间）加密生成。

交易类型标识如下表：

值	含义
01	帐户划入
02	医疗消费

4）.响应报文数据域

说明	长度(字节)

TAC	4
MAC2	4

TAC 是用系统定义的 TAC 子密钥直接对（4 字节的个人帐户交易金额+ 4 字节的个人自付金额+ 4 字节的统筹基金支付金额+1 字节交易类型标识+6 字节终端机编号＋4 字节终端交易序号＋4 字节终端交易日期+3 字节终端交易时间）数据加密生成。

MAC2 由卡中过程密钥对（4 字节的个人帐户交易金额+ 4 字节的个人自付金额+ 4 字节的统筹基金支付金额）数据加密生成。

5）.响应报文状态码

SW1 SW2	意义
90　00	命令正确执行
65　81	写 EEPROM 失败
67　00	长度错误
69　01	命令不接受(无效状态)
69　82	不满足安全状态
69　85	使用条件不满足
6A　81	不支持此功能(无 MF 或 MF 已锁定)
93　02	MAC 无效
93　03	应用永久锁定
94　03	密钥索引不支持

【注】 医疗消费交易完成后，医疗消费交易序号加 1，从 CIA 的旧余额中扣减交易金额，并累计个人自付金额、统筹基金支付金额。此外，在其交易明细文件中存有如下记录：

说明	长度(字节)
医疗消费交易序号	2 字节
交易类型标识	1 字节
终端机编号	6 字节
终端交易日期	4 字节
终端交易时间	3 字节
个人帐户交易金额	4 字节
个人自付金额	4 字节
统筹基金支付金额	4 字节

6.25、 Get Balance 读余额

1）.定义和范围

Get Balance 命令用于读取卡内基本医疗保险个人帐户（CIA）余额/年度个人自付累计金额（SPIP）/年度统筹基金支付累计金额（SPFP）。该命令需验证个人密码（PIN）。

2）.命令报文

代 码	值
CLA	B0
INS	26
P1	00
P2	用于 CIA 用于 SPIP 用于 SPFP
Le	04（P2=01） 06（P2=02 或 03）

3）.命令报文数据域

命令报文数据域不存在。

4）.响应报文数据域

说明	长度(字节)
CIA 余额/ SPIP 余额/ SPFP 余额	4
支付年度（P2=02 或 03）	2

5）.响应报文状态码

SW1 SW2	意义
90　00	命令正确执行
69　82	不满足安全状态
69　85	使用条件不满足
6A　81	不支持此功能(无 MF 或卡片已锁死)
6A　82	文件未找到
6A　86	参数 P1，P2 不正确
93　03	应用永久锁定

6.26、 Get CardData 取卡片数据

1）.定义和范围

Get CardData 命令用于读取卡片中的个人密码剩余错误次数、卡号、卡片剩余空间以及当前状态机。

2）.命令报文

代码	值
CLA	80
INS	CA
P1	00
P2	00—取 PIN 剩余错误次数 01—取卡号 02—取剩余空间地址 03—取当前状态机
Le	01—返回 PIN 错误次数或当前状态机 02—返回卡片剩余空间 08—返回卡号

3）.命令报文数据域

命令报文数据域不存在。

4）.响应报文数据域

PIN 错误次数或当前状态机（Le=01）

卡片剩余空间（Le=02）

卡号（Le=08）

5）.响应报文状态码

SW1 SW2	意义
90 00	命令执行正确
67 00	数据长度错误
6A 86	P1、P2 参数错误
6A 81	不支持此功能(无 MF 或 MF 已锁定)
6A 82	文件未找到

6.27、 Get Transaction Prove 取交易认证

1）.定义和范围

Get Transaction Prove 命令用于取交易认证码（TAC 和 MAC）。它提供了一种在交易处理过程中卡拔出并重插后卡片的恢复机制。

2）.命令报文

代码	值
CLA	B0
INS	2E
P1	00
P2	要取 MAC 或 TAC 所对应的交易类型标识
Lc	02
DATA	要取 MAC 或 TAC 所对应的当前的 CIA 划入或医疗消费交易序号
Le	08

3）.命令报文数据域

说明	长度(字节)
要取 MAC 和 TAC 所对应的 CIA 划入或医疗消费交易序号	2

4）.响应报文数据域

说明	长度(字节)
MAC	4
TAC	4

5）.响应报文状态码

SW1 SW2	意义
90 00	命令正确执行
65 81	写 EEPROM 失败
69 82	不满足安全状态
69 85	使用条件不满足
6A 81	不支持此功能(无 MF 或 MF 已锁定)
6A 82	文件未找到
93 03	应用永久锁定
94 06	所需的 MAC 不可用

【注】防拔功能解释如下：

此功能保证卡片在交易处理过程中的任何情况下（甚至是在更新 EEPROM 过程中掉电的情况下）都能保持数据的完整性。

在终端发给 IC 卡一个命令以更新 CIA 余额时，卡片总会回送一个报文鉴别代码（MAC）或交易验证码（TAC），以证明更新已经发生。一旦余额更新成功，可以通过 Get Transaction Prove 命令获得此 MAC 或 TAC。

如果命令已执行结束，而终端还未收到响应之前，卡片突然拔出，终端将会处于不知卡片是否更新的不定状态。在这种情况下，终端可以用 Get Transaction Prove 命令取回 MAC 或 TAC，如果返回 90 00，则表示卡片更新成功，交易完成。如果不返回 90 00，则表示卡片更新失败，要想完成该交易必须从交易初始化开始重新进行。

6.28、 Update/Get Starting Day 修改/读取年度起始日期

1）.定义和范围

Update/Get Starting Day 命令用于修改或读取医疗保险帐户中的“ 年度起始日期 ” 数据元。修改权限由 DSK 密钥控制。

2）.命令报文

代 码	值
CLA	B0
INS	56
P1	00　修改年度起始日期 01　读取年度起始日期
P2	00
Lc	02（修改年度起始日期时存在）
DATA	见下表（修改年度起始日期时存在）
Le	02（读取年度起始日期时存在）

3）.命令报文数据域

说明	长度(字节)
年度起始日期（格式：mmdd）	2

4）.响应报文数据域

响应报文数据域不存在。

5）.响应报文状态码

SW1 SW2	意义
99　00	命令执行正确
65　81	写 EEPROM 失败
67　00	长度错误
69　01	命令不接受(无效状态)
69　82	不满足安全状态
69　85	使用条件不满足
6A　81	不支持此功能(无 MF 或 MF 已锁定)
6A　86	P1，P2 不正确
93　03	应用永久锁定

7、 安全机制

7.1、 加密算法

SingleDES—密钥长度为 8 字节，数据为 8 字节

加密算法如下：

Y=DES(K)[X]

解密算法如下：

$X=DES^{-1}(K)[Y]$

TripleDES—密钥长度为 16 字节（**K=（K_L||K_R**）），数据为 8 字节

加密算法如下：

$Y=DES(K_L)[DES^{-1}(K_R)[DES(K_L)[X]]]$

解密算法如下：

$Y=DES^{-1}(K_L)[DES(K_R)[DES^{-1}(K_L)[X]]]$

7.2、 密钥管理

7.2.1、 共存应用

为了独立地管理一张卡上不同应用的安全问题，每一个应用应该放在一个单独的 ADF 中，亦即在应用之间应该设计一道“防火墙”，以防止跨过应用进行非法访问。另外，每个应用也不应该与个人化要求和卡中共存的其它应用规则发生冲突。

7.2.2、 密钥的独立性

在 IC 卡中，用于特定功能（如：扣款）的加密/解密密钥不能被任何其它功能所使用，包括保存在 IC 卡中的密钥和用来产生、派生、传输这些密钥的密钥。某些密钥也可以保存在 SAM 中，每一种密钥只能执行特定的功能。

7.2.3、 密钥的生成

密钥必须按照一定的算法在保密、安全的地方生成，例如首先生成主密钥或多级主密钥，然后将主密钥保存在绝对安全的地方（例如 IC 卡中或主机中）。密钥下装时，首先使用主密钥对 IC 卡的特征字节（如应用序号）进行加密（即对主密钥进行分散）生成子密钥（临时存在）。在对主密钥进行分散时，将密钥以明文或密文的形式下装入 IC 卡中，之后临时子密钥消失。整个过程应在保密、安全可靠的方式下进行。

7.2.4、 密钥装载

密钥装载采用安全报文的方式，利用 WRITE KEY 命令来进行。安全报文产生的方式参见命令的说明。

密钥装载的控制过程如下：

- 卡片主控密钥在生产商密钥的控制下装载；

- 卡片主控密钥在卡片主控密钥的控制下更新；
- 卡片维护密钥在卡片主控密钥的控制下装载和更新；
- 应用主控密钥在卡片主控密钥的控制下装载；
- 应用主控密钥在应用主控密钥的控制下更新；
- 应用维护密钥在应用主控密钥的控制下装载和更新；
- 应用主工作密钥在应用主控密钥的控制下装载和更新。

7.2.5、 密钥访问

- 密钥不允许直接读；
- 密钥必须在主控密钥的控制下更新；
- 消费密钥不能被外界直接访问，只能接受内部操作系统发来的进行 MAC 计算的指令，按照指定的流程计算出 MAC；
- 计算临时密钥产生的结果只保留在卡片内部，不能被外界直接访问。

7.2.6、 密钥属性

密钥的使用都有一定的限制，必须满足密钥属性的要求。

密钥属性应包括以下几项：

1）.密钥类型：

密钥类型长度为 1 字节，约定如下：

——00，消费取现密钥

——01，圈存密钥

——02，TAC 密钥

——03，圈提密钥

——04，修改透支限额密钥

——05，应用维护密钥

——06，PIN 解锁密钥

——07，PIN 重装密钥

——08，外部认证（主控）密钥

——09，内部认证密钥

——0A，加密密钥

——0B，个人密码 PIN

——0C，简易钱包应用维护密钥

——0D，超级 PIN

——40，SAM 密钥

——80，用户自定义密钥

2）.密钥算法标识

密钥算法标识指定了密钥所支持加密算法，长度 1 字节。密钥算法标识约定如下：

——0，3DES

——1，DES

——2－255，保留

3）.密钥版本

密钥版本指定某种类型密钥的版本号，长度 1 字节。

4）.密钥分散算法

简称 Diversify，是指将一个双长度的密钥 MK，对分散数据进行处理，推导出一个双长度的密钥 DK。

推导 DK 左半部分的方法是：

- 将分散数据的最右 16 个数字作为输入数据；
- 将 MK 作为加密密钥；
- 用 MK 对输入数据进行 3DEA 运算。

推导 DK 右半部分的方法是：

- 将分散数据的最右 16 个数字求反，作为输入数据；
- 将 MK 作为加密密钥；
- 用 MK 对输入数据进行 3DEA 运算。

7.2.7、 密钥的使用和存放

密钥在使用过程中，每一种密钥只能执行特定的功能，并且采用 Triple DES 使用 16 字节长度的密钥进行加密。在交易过程中，使用临时密钥进行安全交易。密钥在 IC 卡中不应被泄露，也就是说，禁止对密钥进行读操作。

7.2.8、 密钥的终止

每种密钥都有其生命周期，如果卡片被永久锁住，密钥就被终止使用。

7.3、 安全报文

7.3.1、 报文完整性和验证

MAC 是使用命令中的所有的元素（包含命令头）产生的。MAC 是命令数据域中最后一个数据元，它的长度为 4 个字节。

MAC 的计算方法如下：

第一步：

终端向 IC 卡发出一个 Get Challenge 命令，在 IC 卡回送的 4 字节随机数后缀以‘ 00 00 00 00 ’，所得到的结果作为初始值。

第二步：

按照顺序将以下数据连接在一起形成数据块：

——CLA，INS，P1，P2，Lc+4，Data

——必须置 CLA 的后半字节为‘ 4 ’

——在命令的数据域中（如果存在）包含明文或加密的数据

第三步：

将该数据块分成 8 字节为单位的数据块，标号为 D1，D2，D3，D4 等，最后的数据块有可能是 1-8 个字节。

第四步：

如果最后的数据块长度是 8 字节的话，则在其后加上 16 进制数字‘ 80 00 00 00 00 00 00 00 ’，转到第五步。如果最后的数据块长度不足 8 字节的话，则在其后加上 16 进制数字‘ 80 ’，如果达到 8 字节长度，则转入第五步；否则在其后加入 16 进制数字‘ 0 ’直到长度达到 8 字节。

第五步：

对这些数据块使用相应的密钥进行加密。根据密钥的长度采用 Single DES 或 Triple DES。

Triple DES 的加密方法如下图所示：

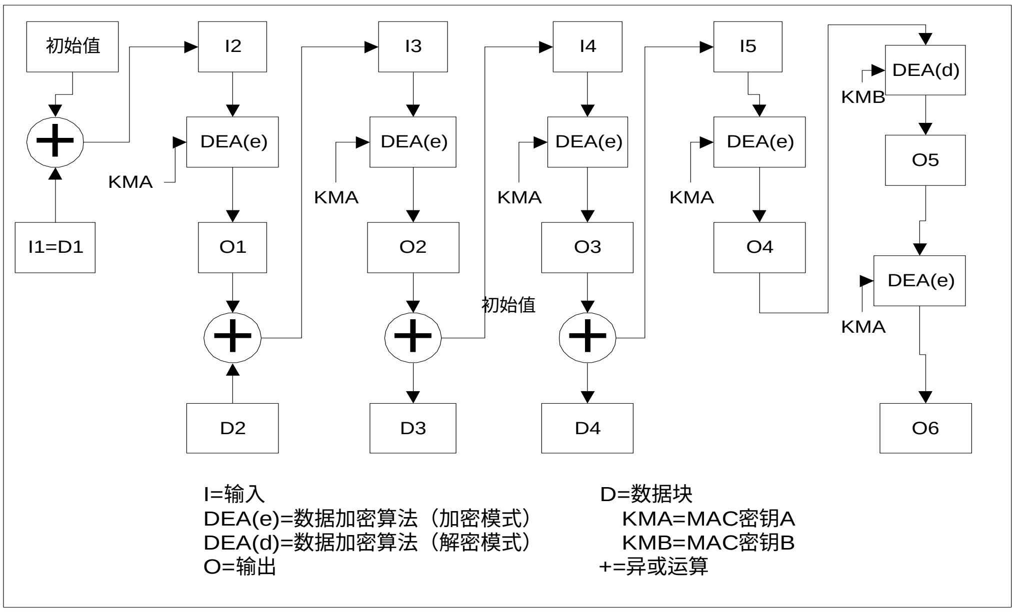


图 7.3.1 Triple DES 的 MAC 算法

第六步：

最终得到是从计算结果左侧取得的 4 字节长度的 MAC。

7.3.2、 安全报文传送的命令情况

在 ISO/IEC7816-4 中定义了四种命令情况。

情况一：

这种情况时，没有数据送到 ICC（L_C）中，也没有数据从卡中返回（Le)。

没有安全报文传送要求的命令情况如下：

CLA	INS	P1	P2

有安全报文传送要求的命令情况如下：

CLA	INS	P1	P2	L_C	MAC

CLA 的第二个半字节是‘4’表明支持第二种情况的安全报文传送。L_C 为 MAC 的长度。

情况二：

这种情况时，命令中没有数据送到卡中，但有数据从卡中返回。没有安全

报文传送要求的命令情况如下：

CLA	INS	P1	P2	Le

有安全报文传送要求的命令情况如下：

CLA	INS	P1	P2	Lc	MAC	Le

CLA 的第二个半字节是‘4’表明支持第二种情况的安全报文传送。L_C 为 MAC 的长度。

情况三：

这种情况时，命令中有数据送到卡中，但没有数据从卡中返回。没有安全报文传送要求的命令情况如下：

CLA	INS	P1	P2	L_C	命令数据

有安全报文传送要求的命令情况如下：

CLA	INS	P1	P2	Lc	命令数据	MAC

CLA 的第二个半字节是‘4’表明支持第二种情况的安全报文传送。L_C 为命令数据加上 MAC 的长度。

情况四：

这种情况时，在命令中有数据送到卡中，也有数据从卡中返回。没有安全报文传送要求的命令情况如下：

CLA	INS	P1	P2	L_C	命令数据	Le

有安全报文传送要求的命令情况如下：

CLA	INS	P1	P2	Lc	命令数据	MAC	Le

CLA 的第二个半字节是‘4’表明支持第二种情况的安全报文传送。L_C 为命令数据加上 MAC 的长度。

7.4、 数据的加、解密计算

7.4.1、 数据加密计算

数据加密步骤如下：

第一步：

用 L_D 表示明文数据的长度，在明文数据前加上 L_D 产生新数据块。

第二步：

将第一步中生成的数据块分解成 8 字节数据块，标号为 D1，D2，D3，D4 等等。最后一个数据块的长度有可能不足 8 位。

第三步：

如果最后（或唯一）的数据块长度等于 8 字节，转入第四步；如果不足 8 字节，在右边添加 16 进制数字‘80’。如果长度已达 8 字节，转入第四步；否则，在其右边添加 1 字节 16 进制数字‘0’直到长度达到 8 字节。

第四步：

对每个数据块用相应的密钥进行加密，根据密钥的长度可以使用 SingleDES 或 TripleDES。

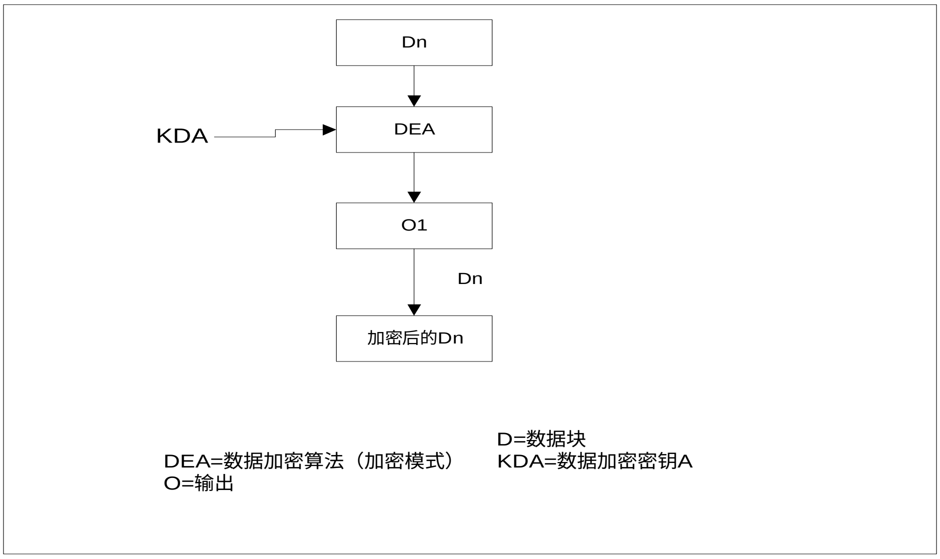


图 7.4.1 使用 SingleDES 的数据加密

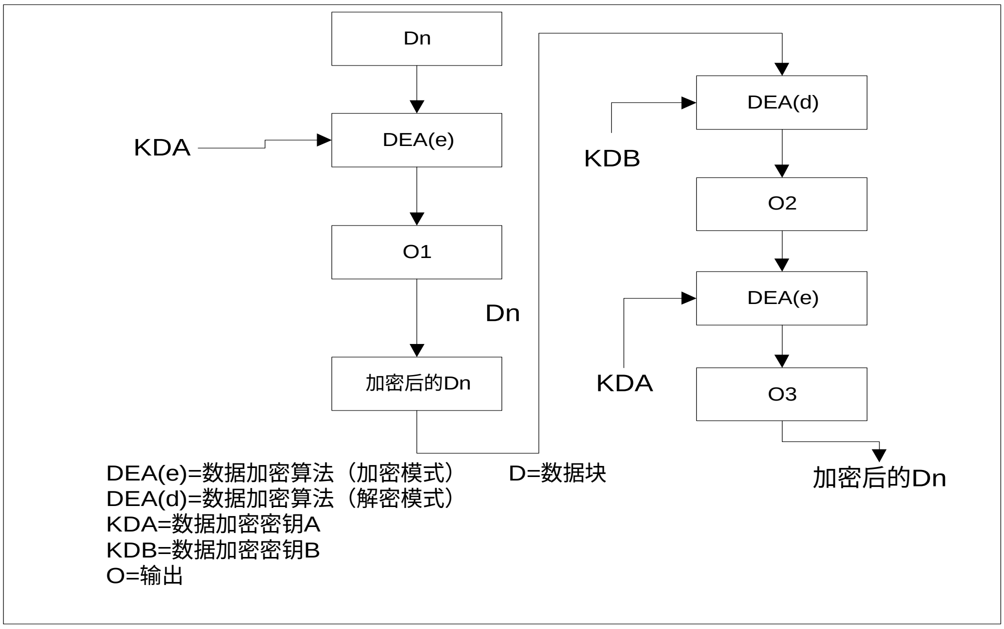


图 7.4.2 使用 TripleDES 的数据加密

第五步：

计算结束后，所有加密后的数据块依照原顺序连接在一起（加密后的 D1，加密后的 D2，等等），并将结果数据块插入到命令数据域中。

7.4.2、 数据解密计算

数据解密步骤如下：

第一步：

将命令数据域中的数据块分解成 8 字节长的数据块，标号为 D1，D2，D3，D4 等等。每个数据块使用如下过程进行解密。

用与加密相同的密钥进行解密，SingleDES 和 TripleDES 的解密过程如图 7.4.3 所示：

如果采用双长度数据加密的 DEA 密钥，则数据块的解密如图 7.4.4 所示（使用数据加密过程密钥 A 和 B 来进行解密）。

第二步：

计算结束后，所有解密后的数据块依照顺序（解密后的 D1，解密后的 D2，

等等）链接在一起。数据块由 L_D，明文数据，填充字符组成。

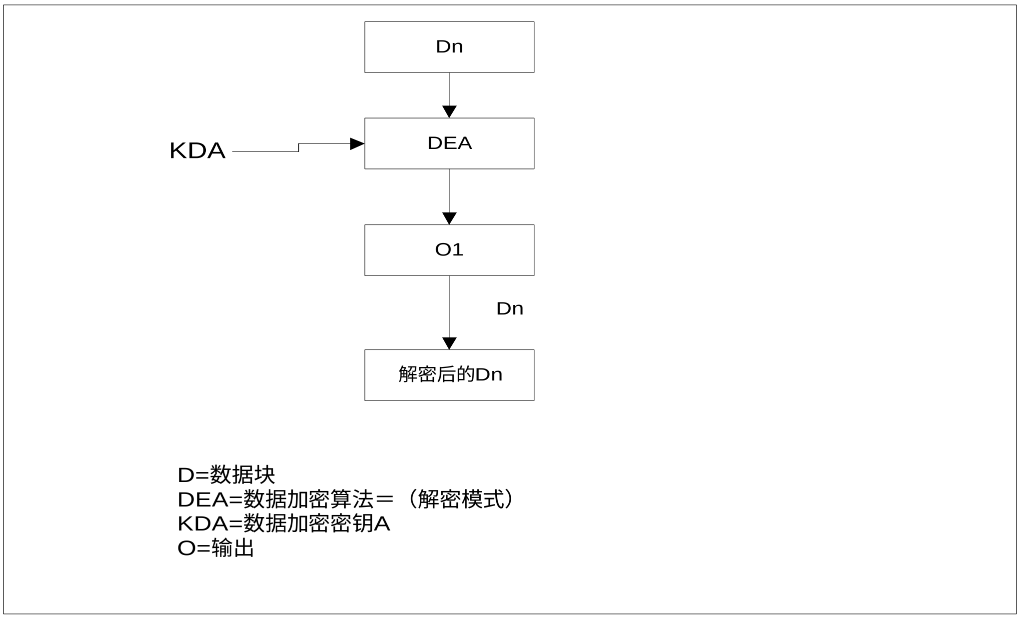


图 7.4.3 使用 SingleDES 的数据解密

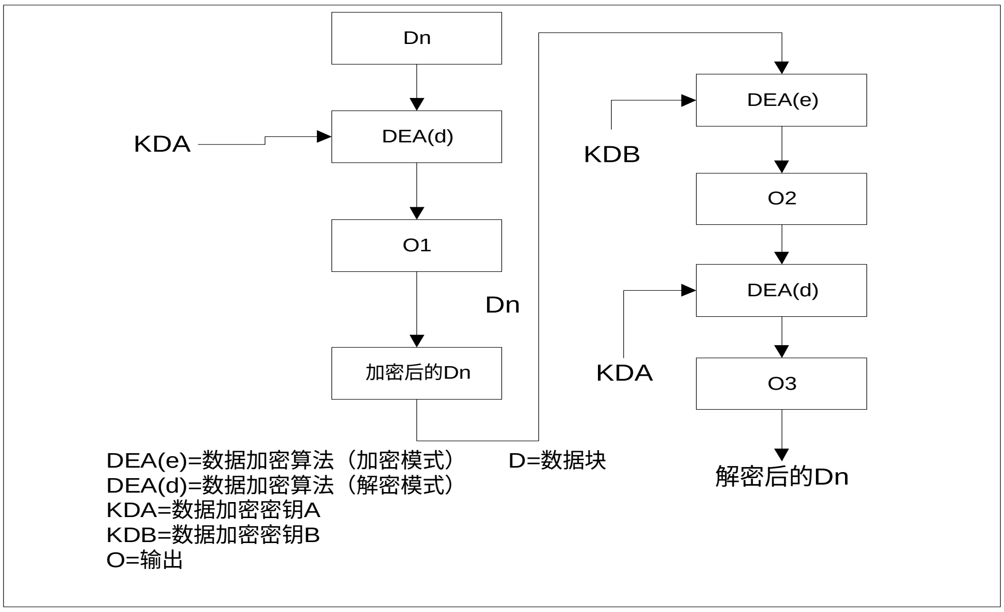


图 7.4.4 使用 Triple DES 的数据解密

第三步：

因为 L_D 表示明文数据的长度，因此，它被用来恢复明文数据。

7.5、 ED/EP 应用的密钥关系

7.5.1、 密钥关系表

密钥	发卡方	IC 卡	POS（PSAM）
用于医疗消费的密钥	医疗消费主密钥（MPK）	医疗消费子密钥（DPK），由 MPK 用应用序列号推导获得	消费主密钥（MPK）
用于帐户划入交易的密钥	帐户划入主密钥（MLK）	帐户划入子密钥（DLK），由 MLK 用应用序列号推导获得	N/A
中用于产生交易 TAC 的密钥	TAC 主密钥（MTK）	TAC 子密钥（DTK），由 MTK 用应用序列号推导获得	N/A
用于解锁 PIN 的密钥	PIN 解锁主密钥（MPUK）	PIN 解锁子密钥（DPUK），由 MPUK 用应用序列号推导获得	由发卡方考虑决定

7.5.2、 子密钥推导方法

下面是 IC 卡中密钥的推导方法。图 7.5.1 和图 7.5.2 描述了 DPK 的推导过程。

推导双倍长 DPK 左半部分的方法：

——将应用序列号的最右 16 个数字作为输入数据

——将 MPK 作为加密密钥

——用 MPK 对输入数据进行 Triple DES 运算

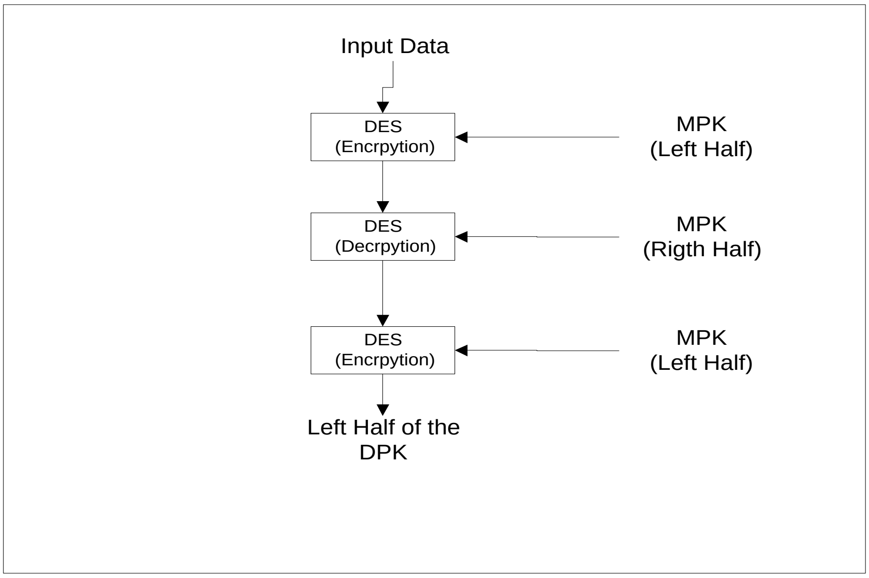


图 7.5.1 DPK 左半部分的推导过程

推导双倍长 DPK 右半部分的方法：

——将应用序列号的最右 16 个数字的求反作为输入数据

——将 MPK 作为加密密钥

——用 MPK 对输入数据进行 TripleDES 运算

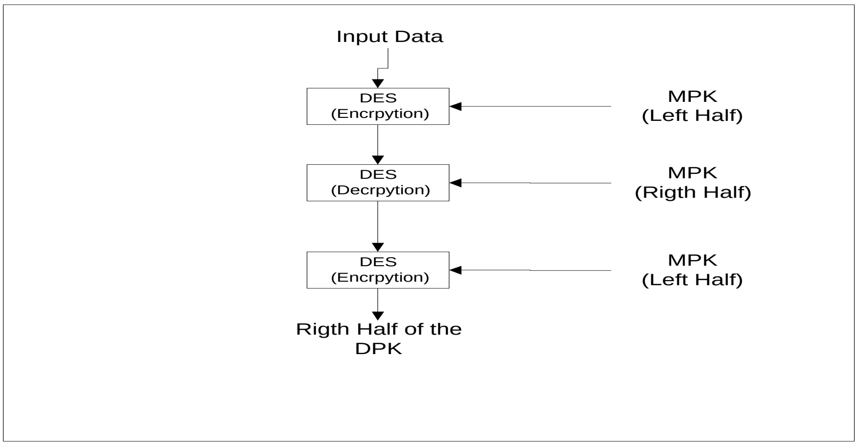


图 7.5.2 DPK 右半部分的推导过程

7.5.3、 过程密钥的产生

过程密钥是在交易过程中用可变数据产生的单倍长密钥。过程密钥产生后只能在某过程/交易中使用一次。

图 7.5.3 描述了产生过程密钥的机制。这方法也用于不同交易类型的过程密钥的产生，输入的数据是随机数。

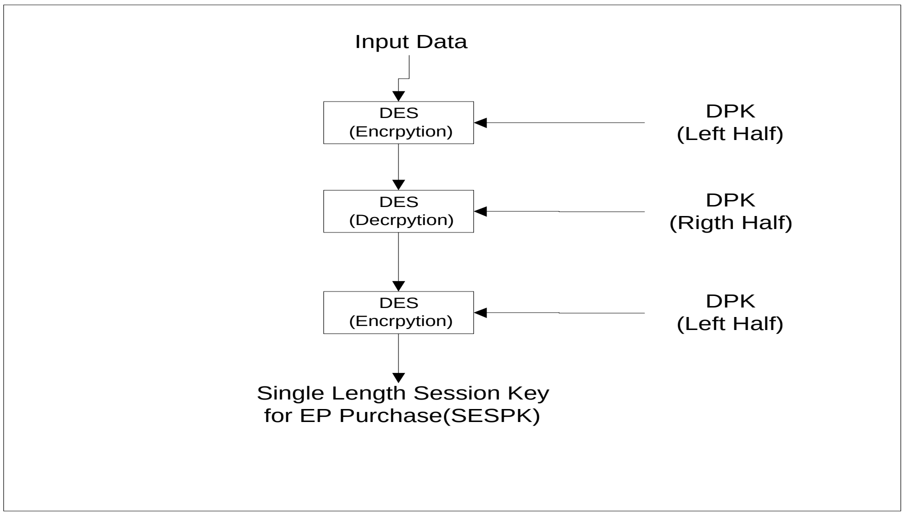


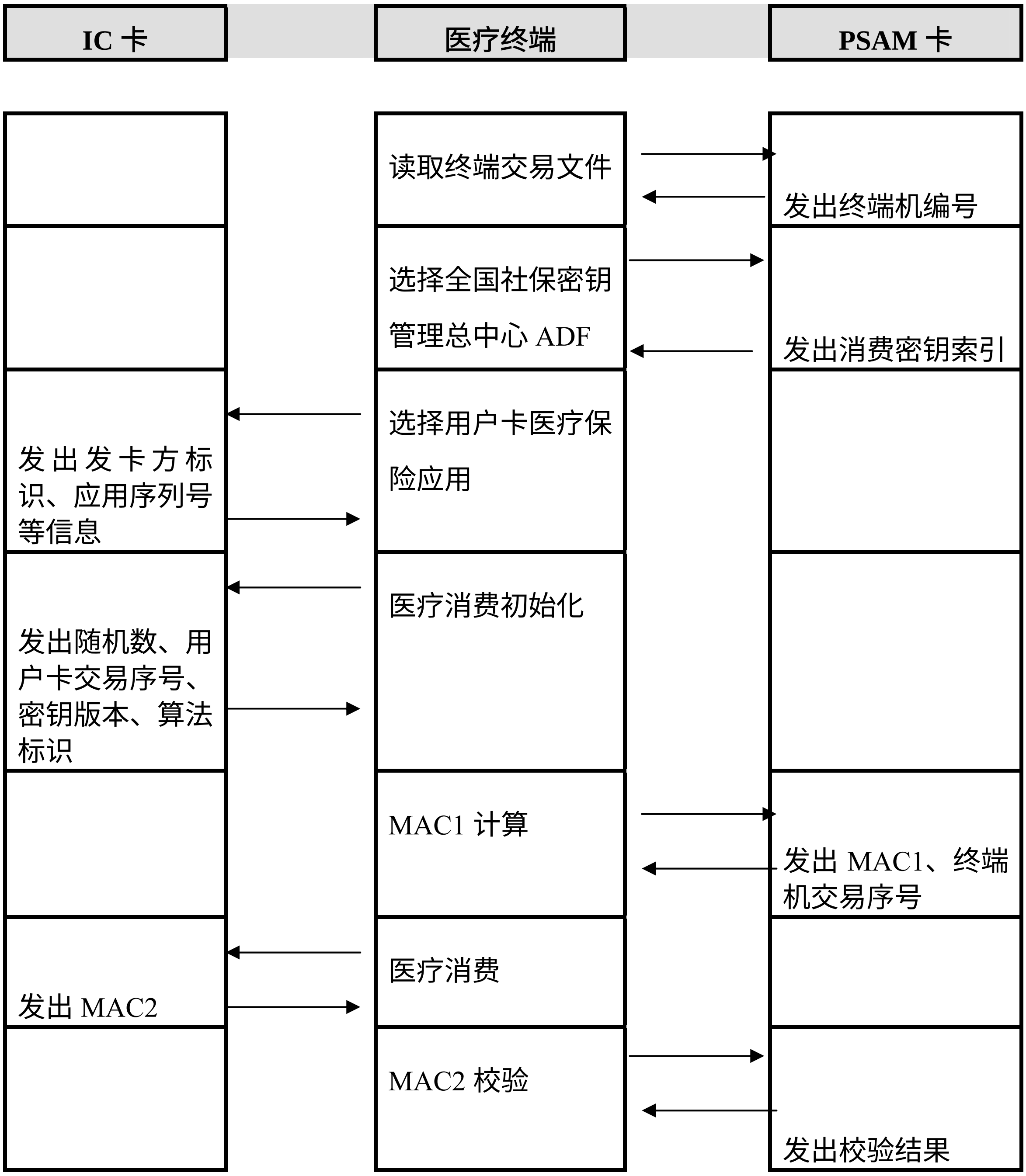
图 7.5.3 过程密钥的产生

8、用户卡发卡流程

- 在 IC 卡生产过程中，IC 卡生产厂商在卡中设置生产商密钥（kMprd），控制 IC 卡的安全运输，以防止在 IC 卡生产商和发卡行机构间被人替换。在将 IC 卡交给发卡机构的同时，也将装有生产商密钥的母卡交给发卡机构。
- 发卡机构接到这一批 IC 卡后，首先按统一编号给每张 IC 卡分配母卡序列号（ASN）。每张 IC 卡具有唯一的 ASN，不同的 IC 卡具有不同的 ASN。
- PC 向高速发卡机发指令，送入一批卡片，利用生产商母卡上的 kMprd 来验证 IC 卡。
- 如验证通过，加载发卡机构的的主控密钥 kIctlM，用 kMprd 对 kIctlM 加密，将密文 3DES（kMprd，kIctlM）载入 IC 卡，在 IC 卡内部使用 kMprd 解密密文，$3DES^{-1}$（kMprd，3DES（kMprd，kIctlM）），还原得到 kIctlM。
- 在 kIctlM 的控制下，创建 MF 下的 EF 文件，并加载应用主控密钥 kActl，写入卡中。
- 在 kActl 的控制下，创建 ADF 下的文件，写入卡片子密钥。
- 在卡上打印应用序列号。
- 如果在写卡或打印卡号的过程中，出现错误，则将卡片作废，重新制作一张同样卡号的卡片。

9、医疗消费交易流程

医疗终端利用 PSAM 卡进行医疗消费交易的处理流程如下图所示：



消费交易流程